

Measuring Public Wi-Fi Security Awareness via Captive Portal Connections Using a Microcontroller

Hyago Santana Mariano *, Daniel Chaves Café *

*Professional Graduate Program in Electrical Engineering - PPEE,
Department of Electrical Engineering – University of Brasília (UnB)
Email: hyago.mariano@aluno.unb.br, daniel.cafe@unb.br

Abstract—This article proposes the implementation of a captive portal system on a microcontroller to assess users' maturity regarding the safe use of public Wi-Fi networks. The use of public Wi-Fi networks has become increasingly common in places like cafes, airports, shopping centers, and hotels. However, many users are unaware of the risks associated with using these unsecured networks, such as personal information theft, privacy invasion, and cyberattacks. This study aims to utilize a microcontroller to generate a signal mimicking a known public network, where, upon user login, an educational authentication portal will be displayed. This portal will not only provide information about security risks but also evaluate the users' maturity level in adopting safe practices on public Wi-Fi networks, offering guidelines on how to protect their data and devices.

Keywords—Cybersecurity, Public Wi-Fi Networks, Captive Portal, Security Awareness, Man-in-the-Middle Attacks.

I. Introduction

The rapid expansion of public Wi-Fi networks has provided greater convenience and internet access in places like cafes, airports, hotels, and public squares. However, this ease of access also brings significant information security risks. Cyberattacks, such as Man-in-the-Middle (MITM) attacks, have become increasingly sophisticated and pose a serious threat to users of unprotected Wi-Fi networks.

Given this scenario, it is crucial to assess the information security maturity of these network users to identify potential vulnerabilities and raise awareness about best security practices. This study proposes the creation of a captive portal using a microcontroller to simulate a fake public Wi-Fi network. This approach will allow for measuring users' preparedness regarding cyber threats.

The captive portal is a widely used technique for authentication and access management in public Wi-Fi networks. It offers users a login page where it is

required to provide credentials or agree to terms of use before accessing the internet. In this study, we will use a microcontroller to create a simulated environment where a captive portal will be deployed to emulate a public Wi-Fi network.

The central idea of the study is to check if people will connect to this fake network, believing it to be a legitimate public Wi-Fi network. By analyzing this interaction, we can gain valuable insights into user awareness and behavior concerning cyber threats on public Wi-Fi networks. Additionally, this approach will allow us to identify knowledge gaps and provide insights on how to improve information security in this context.

The primary goal of this work is to educate and promote good security behaviors in open public networks. To achieve this, we developed an informational captive portal designed to mimic a specific public Wi-Fi network, highlighting common security risks and providing educational content to users.

To achieve this goal, this work also proposes: (a) Evaluating the behavior of users when connecting to public Wi-Fi networks and identifying their perceptions about cybersecurity. (b) Analyzing the effectiveness of an educational captive portal in raising awareness of the security risks associated with public Wi-Fi networks. (c) Measuring the cybersecurity maturity of users and identifying knowledge gaps and risky behaviors. (d) Developing and proposing recommendations to enhance user security and awareness when using public Wi-Fi networks, based on observed behaviors and vulnerabilities. (e) Proposing a replicable methodology for assessing cybersecurity maturity in public networks using microcontrollers and educational portals.

Objective (a) aims to evaluate user behavior when connecting to public Wi-Fi networks and identify their perceptions of cybersecurity. This is covered primarily in Section III – Methodology and Section IV – Results. Section III outlines the experimental setup and

development of the captive portal used to simulate a public network, facilitating the observation of user interactions. Section IV presents test results, emphasizing user perceptions of cybersecurity and the types of behaviors observed.

Objective (b) seeks to analyze the effectiveness of an educational captive portal in raising user awareness of security risks in public Wi-Fi networks. It is discussed in Section I – Introduction, Section III – Methodology, and Section IV – Results. Section I provides the context for developing the portal as an educational tool, while Section III details its implementation and content. Section IV evaluates the portal’s impact on user behavior and understanding of security risks.

Objective (c) aims to measure users’ cybersecurity maturity and identify knowledge gaps and risky behaviors. This is covered in Section IV – Results and Section V – Summary of Findings. Section IV assesses participant responses and their cybersecurity maturity, highlighting risky behaviors and gaps in knowledge. Section V consolidates these findings and discusses the primary knowledge gaps observed.

Objective (d) focuses on developing recommendations to enhance user security and awareness based on observed behaviors and vulnerabilities. This is addressed in Section V – Summary of Findings and Section VI – Conclusions. Section V proposes recommendations based on the results, suggesting practices for users to adopt when using public networks. Section VI reinforces these recommendations and offers additional guidelines for organizations providing public Wi-Fi.

Objective (e) suggests a replicable methodology for assessing cybersecurity maturity using microcontrollers and educational portals. This is detailed in Section III – Methodology and Section VI – Conclusions. Section III describes the development and implementation of the methodology using the esp32 microcontroller, while Section VI discusses its application in different contexts and highlights the potential for future research.

II. Related Works

Social engineering is a widely used technique by hackers to obtain confidential information or illegally access computer systems. According to [1], user awareness and training are essential for preventing and combating social engineering. Investing in employee training programs can significantly reduce the risk of such attacks. Additionally, measures such as access control, network monitoring, and security audits are recommended to protect systems and information.

Ali et al. [2] address the privacy risks associated with using public Wi-Fi networks with captive portals.

They highlight that the authentication process can be exploited to collect sensitive user information, such as login data and passwords, through phishing techniques. The empirical study demonstrated that many users provide personal information without verifying network security, highlighting the vulnerability in public networks and reinforcing that the weakest link in security is often the user themselves.

Studies conducted by Vaccari et al. [3] show that Wi-Fi-enabled devices have exploitable vulnerabilities that attackers can use to execute malicious code. The research indicates that compromised IoT devices can propagate attacks throughout the network, underscoring the importance of awareness and implementing security measures to mitigate these risks.

Hammad and Ati [4] identified phishing and data interception vulnerabilities in public Wi-Fi networks in the United Arab Emirates. The study suggests adopting preventive measures, such as strong authentication and using virtual private networks (VPNs), to ensure network security.

Sombatruang et al. [5] conducted research in Japan, showing that most users are unaware of the security risks associated with public networks. Even when aware, many continue using these networks for convenience. The research underscores the need for user awareness and the adoption of additional security measures to protect against attacks on public Wi-Fi networks.

Bauer et al. [6] propose an authentication system that uses SSL certificates and an authentication server to mitigate Evil Twin attacks. The system allows users to verify the network’s identity before connecting, achieving a 100% detection rate in their experimental tests.

In the academic context, internet connectivity is essential for research, teaching, and administration. The University of Brasília (UnB), with a community of over 50,000 people, relies heavily on public Wi-Fi networks for access to online resources. Ensuring the security of these networks is a challenge, given the potential vulnerabilities and the need to protect sensitive information and institutional reputation. Measuring cybersecurity maturity is essential to assess the effectiveness of implemented security measures and identify areas for improvement.

The Cyber Security Body of Knowledge (CyBOK), in the chapter on Human Factors by Sasse and Rashid [7], highlights the importance of aligning security policies with human capabilities and limitations, emphasizing that security measures are only effective if they are usable and appropriate for users’ contexts. This principle underpins the approach of the present study, which

utilizes captive portals on public Wi-Fi networks as an educational tool. By simulating risk scenarios on a public network and embedding security awareness elements, the study aims to bridge the gap between users' risk perception and the adoption of practical protective measures, as discussed in CyBOK. This approach not only encourages responsible use of public networks but also reinforces the need for policies and educational campaigns that increase users' familiarity with accessible and applicable security practices.

Sun et al. [8] conducted a comprehensive survey on privacy and security issues in IoT-based environments, examining the unique challenges faced in these systems. Their study outlines a systematic approach to identifying vulnerabilities across different layers of IoT networks, including the perception, network, and application layers. The authors emphasize the significance of secure communication protocols and the implementation of robust access control mechanisms to prevent unauthorized access and data breaches. Additionally, the survey addresses the role of emerging technologies, such as blockchain and artificial intelligence, in mitigating these risks. Sun et al. further propose future research directions that include the development of post-quantum cryptographic algorithms and AI-driven security models to adapt to the evolving landscape of IoT threats.

III. Methodology

The research was conducted in the courtyard of the Faculty of Gama (FGA) at the University of Brasília (UnB), a location frequented by students, teachers, and staff, making it ideal for conducting an educational campaign on cybersecurity. The choice of the FGA courtyard allowed for reaching a diverse audience, composed of individuals with different levels of knowledge in digital security, expanding the educational impact of the initiative.

For this experiment, a public Wi-Fi network with the same SSID as the genuine network of the University of Brasília was created, prompting users to connect to the unauthenticated network. The objective was to set an environment to analyze users' susceptibility to cyberattacks, such as potential theft of personal data and passwords, without actually conducting such attacks.

After users connected to the fake network, they were redirected to a home page that requested authentication, similar to common free Wi-Fi networks found in public places. This login page simulated a captive portal, a technique often used to capture login credentials and other sensitive information. After entering the credentials, users were redirected to an awareness

page that explained the simulated attack and offered guidance on how to protect themselves against such threats in the future.

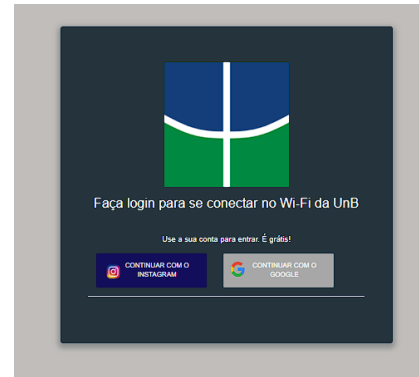


Figure 1: Captive Portal Login

Participants learned about the dangers associated with using unsecured public Wi-Fi networks through the information provided on the awareness page. They were instructed on secure connection practices, such as using virtual private networks (VPNs), two-factor authentication, and checking security certificates. This approach aimed to raise collective awareness and encourage the academic community to adopt proactive measures to protect their data and privacy.

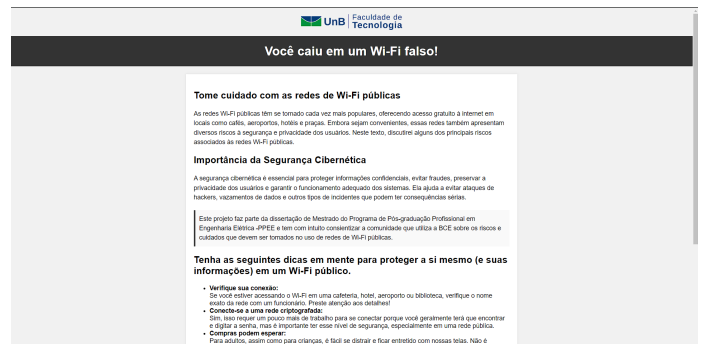


Figure 2: Cyber Security Awareness Page

The experiment used an ESP32 module with an OLED shield, SD storage, external antenna, and a rechargeable battery connected via mini USB, enhancing portability. The ESP32, a powerful, low-cost microcontroller popular in IoT projects, offers strong processing power and Wi-Fi/Bluetooth connectivity. For replicating real-world attack scenarios, the compact ESP32 with an external antenna provides extended range and robust signal strength, ideal for high-traffic areas. The SD board hosted files for the captive portal, creating a realistic test setup. This configuration allows for covert, prolonged deployment, effectively simulat-

ing the setup of rogue access points aimed at attracting unsuspecting users.

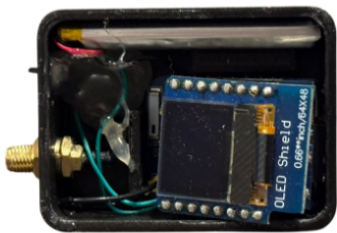


Figure 3: ESP32 Module

The test environment was configured to ensure that the experiment did not violate the real privacy of users. No information collected was used for malicious purposes, and users were informed about the experiment after the initial interaction as part of the educational process.

The data were collected anonymously through a 14-question form using a Likert scale, designed to measure users' perceptions and attitudes towards cybersecurity. The objective of the form was to evaluate participants' understanding of the risks associated with using public Wi-Fi networks and assess their behavior when interacting with a network that used the same SSID as the original one. By capturing varying levels of agreement or disagreement, the Likert scale enabled a detailed assessment of users' awareness, reactions to the fake network, and potential susceptibility to cyber threats.

Participants were also informed about the study's purpose, data confidentiality, and voluntary participation through an Informed Consent Declaration, ensuring ethical compliance and reliable data collection for evaluating the impact of the educational campaign.

These metrics provided valuable information on users' awareness and behavior regarding cyber threats present in public Wi-Fi networks, highlighting the need for ongoing educational interventions to promote more robust security practices.

IV. Results

The study results are organized into key areas that highlight participants' perceptions and behaviors towards public Wi-Fi networks:

A. Understanding of Phishing Risks

Only 34% of participants expressed concern about phishing on public Wi-Fi networks, with a considerable proportion remaining undecided (37%) or unconcerned (29%). This indicates a gap in understanding the specific risks associated with phishing attacks.

B. Awareness of Security Certificates

The data indicate a lack of concern for security certificates when accessing sites that request personal information. A significant portion of participants (46%) reported that they *almost never* check for security certificates, while 12% stated that they *never* do so. On the other hand, only 10% check *almost always*, and none indicated *always* checking. This behavior highlights a critical gap in awareness and a potential vulnerability to phishing attacks or malicious websites.

C. General Perception of Public Wi-Fi Security

The majority of participants (56%) perceive public Wi-Fi networks as "very insecure" while 39% consider them "insecure." Only a small percentage viewed these networks as "neutral" (2%) or "secure" (2%). This indicates a widespread concern about security risks associated with public Wi-Fi use.

D. Preparedness Against Man-in-the-Middle (MITM) Attacks

A substantial proportion of participants (54%) did not express fear of MITM attacks, with 41% remaining undecided. This suggests limited awareness or understanding of the threats posed by MITM attacks, even though these are prevalent risks in public Wi-Fi environments.

E. Awareness of Spoofing and Malware Risks

The majority of respondents (68%) were undecided about the risk of spoofing (network forgery), while 44% were undecided about the possibility of malware or virus infection. This lack of clarity reflects a need for better education on these specific cyber threats.

F. Concerns Over Government and Corporate Data Collection

A significant number of respondents (64%) believe their information might be collected or monitored by the government or corporations when using public Wi-Fi. This reflects high awareness of privacy risks, although specific protective measures are not always taken.

G. Perception of Data Theft Risk

The results show that 81% of respondents are aware that their data could be stolen on public Wi-Fi networks due to inadequate encryption. Of these, 27% "strongly agreed" and 54% "agreed." However, 15% were "undecided," and only 4% disagreed. This suggests that while most users recognize the risk, there is still a gap in translating awareness into protective actions, such as using VPNs or avoiding sensitive activities on these networks.

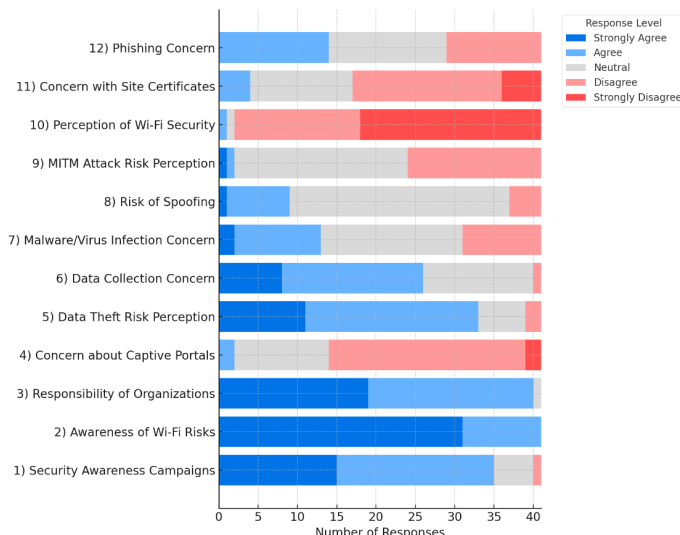


Figure 4: Survey Results: Perceptions and Concerns About Risks of Public Wi-Fi Networks

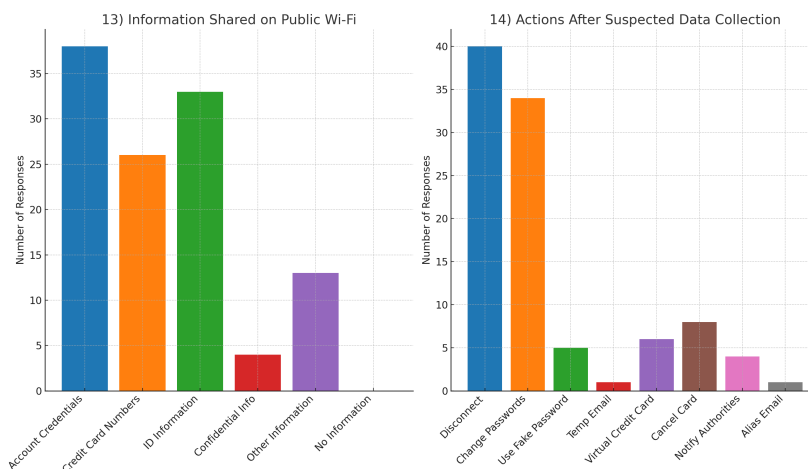


Figure 5: Survey Results: Perceptions and Concerns About Risks of Public Wi-Fi Networks

H. Concern Over Captive Portal Authenticity

Most participants (61%) were not concerned about the authenticity of captive portals in public Wi-Fi environments, such as those found in airports, hotels, and cafes. Only 5% expressed concern, suggesting a lack of awareness about potential security threats posed by these portals.

I. Response Actions to Potential Information Breach

When asked about potential responses to a suspected breach, most participants (97%) would disconnect from the network, and 83% would change their passwords. However, fewer would take additional protective actions, indicating a limited preparedness for comprehensive incident response.

J. Perception of Security in Various Public Locations

Participants generally perceived public Wi-Fi networks in cafes, airports, shopping malls, and universities as "unsafe" (59%) or "very unsafe" (24%), reinforcing the overall sentiment of insecurity.

K. General Perception of Security in Public Wi-Fi Networks

The research revealed a significant perception of insecurity among users of public Wi-Fi networks. Of the 41 respondents, 95% consider these networks unsafe, with 56% rating them as "very unsafe." This data highlights a broad awareness of the potential risks associated with using public networks, where encryption and authenticity are not always guaranteed.

L. Need for Increased Awareness Efforts

All participants (100%) agreed that there should be more widespread efforts to raise awareness about the risks of public Wi-Fi networks, emphasizing the importance of educational campaigns and resources.

M. Types of Information Shared

Users often share sensitive information on public Wi-Fi networks. About 93% of respondents admitted to sharing online account credentials, and 80% shared credit card information. Additionally, 80% reported sharing personal identification details (e.g., CPF and RG), and 10% disclosed sharing confidential or corporate data. This behavior underscores a significant vulnerability in handling sensitive information.

V. Conclusions and Future Work

The educational campaign to raise awareness about security risks in public Wi-Fi networks, conducted on the University of Brasília (UnB) campus with an embedded captive portal, proved an effective strategy for informing users about the associated threats and promoting strong cybersecurity practices. Using the ESP32 microcontroller, the study created a simulated public network environment, allowing users to experience realistic risk scenarios and reinforcing the importance of secure navigation.

Research findings indicated that while users generally perceive public Wi-Fi networks as insecure, this awareness seldom leads to proactive security measures. Participants exhibited limited understanding of protective strategies, such as VPN use, two-factor authentication, and verifying security certificates. This gap between risk perception and specific security practices highlights the need for more detailed, targeted awareness campaigns.

Moreover, the continued exposure of personal data by users on public networks, despite knowledge of potential risks, underscores the importance of not only raising awareness of threats but also educating on practical security behaviors applicable to daily use. Many users expressed a desire for public Wi-Fi providers to take a more active role in promoting secure practices, suggesting a need for policies that prioritize user safety alongside internet access.

The study emphasizes the value of developing educational campaigns focused on raising awareness of risks and foundational protective practices, including workshops, interactive resources, and hands-on sessions. These initiatives allow users to experience risk scenarios and learn practical ways to identify and respond to threats. By enhancing this foundational cybersecurity

knowledge, a stronger digital security culture can be fostered among public Wi-Fi users.

The use of affordable microcontrollers like the ESP32 shows promise for awareness simulations, with potential for broader application in reaching diverse audiences. This study highlights key gaps in user behavior and security awareness, providing practical steps to bridge them. Strengthening cybersecurity education in public networks is essential to create a safer online environment. These findings support future research, educational efforts, and policy initiatives to improve cybersecurity in public Wi-Fi settings.

References

- [1] J. Guarezi, "Engenharia social: avaliação de riscos e vulnerabilidades tendo o fator humano como o elo mais fraco da segurança da informação," *Sistemas de Informação-Pedra Branca*, 2019.
- [2] S. Ali, T. Osman, M. Mannan, and A. Youssef, "On privacy risks of public wi-fi captive portals," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26-27, 2019, Proceedings 14*. Springer, 2019, pp. 80–98.
- [3] I. Vaccari, S. Narteni, M. Mongelli, M. Aiello, and E. Cambiaso, "Perpetrate cyber-attacks using iot devices as attack vector: The esp8266 use case," in *CEUR Workshop Proceedings*, vol. 2940, 2021, pp. 35–46.
- [4] L. A. Hammad and M. Ati, "Assessing security health of public wi-fi environments in the uae," in *2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*. IEEE, 2020, pp. 1–6.
- [5] N. Sombatruang, Y. Kadobayashi, M. A. Sasse, M. Baddeley, and D. Miyamoto, "The continued risks of unsecured public wi-fi and why users keep using it: Evidence from japan," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018, pp. 1–11.
- [6] K. Bauer, H. Gonzales, and D. McCoy, "Mitigating evil twin attacks in 802.11," in *2008 IEEE International Performance, Computing and Communications Conference*. IEEE, 2008, pp. 513–516.
- [7] M. A. Sasse and A. Rashid, "The cyber security body of knowledge: Human factors knowledge area," The National Cyber Security Centre, 2021, version 1.0.1, © Crown Copyright, The National Cyber Security Centre 2021, licensed under the Open Government Licence: <http://www.nationalarchives.gov.uk/doc/open-government-licence/>. [Online]. Available: <https://www.cybok.org>
- [8] P. Sun, Y. Wan, Z. Wu, Z. Fang, and Q. Li, "A survey on privacy and security issues in iot-based environments: Technologies, protection measures and future directions," *Computers Security*, vol. 148, p. 104097, 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404824004024>
- [9] P. Sun, S. Alqahtani, F. Z. Yousaf, and H. Otrok, "A survey on privacy and security issues in iot-based environments," *Journal of Network and Computer Applications*, vol. 14, no. 2, pp. 105–120, 2024.