

Prevention Of Cyber Attacks On Home WiFi Network

BY

Gopal Chandra Deb

ID: 221-25-136

This Report Presented in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science and Engineering

Supervised By

Dr. Touhid Bhuiyan

Professor & Head

Department of CSE

Daffodil International University

Co-Supervised By

Abdus Sattar

Assistant Professor

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY


DHAKA, BANGLADESH

JANUARY 2023

APPROVAL

This Project/Thesis titled “**Prevention Of Cyber Attacks On Home WiFi Network**”, submitted by **Gopal Chandra Deb**, ID No: **221-25-136** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 17-01-2023.

BOARD OF EXAMINERS

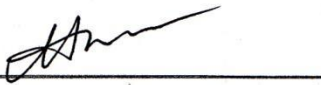


Dr. Touhid Bhuiyan, PhD

Professor and Head

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman

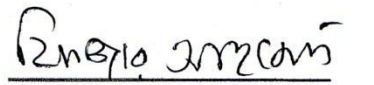


Ms. Nazmun Nessa Moon

Associate Professor

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Fizar Ahmed

Associate Professor

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Md. Safaet Hossain

Associate Professor & Head

Department of Computer Science and Engineering
City University

External Examiner

DECLARATION

I hereby declare that this thesis has been done by me under the supervision of **Dr. Touhid Bhuiyan, Professor and Head, Department of CSE**, Daffodil International University. I also declared that neither this thesis nor any part of this thesis has been submitted elsewhere for the award of any degree or diploma.

Supervised by:

Dr. Touhid Bhuiyan



Professor & Head
Department of CSE
Daffodil International University

Co-Supervised by:

Abdus Sattar



Assistant Professor
Department of CSE
Daffodil International University

Submitted by:

Gopal Chandra Deb



Student
ID: 221-25-136
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First and foremost, I would like to express my heartfelt gratitude to Almighty God for His wonderful grace, which has enabled me to successfully finish my final year thesis.

I worked hard on this thesis. However, without the kind help and support of many individuals, it would not be possible. I want to express my sincere thanks to each and every one of them.

I owe a tremendous amount of gratitude to Daffodil International University for their direction and continual supervision, as well as for the provision of vital information about the thesis and for their assistance in concluding the thesis.

I would like to take this opportunity to thank my supervisor, **Dr. Touhid Bhuiyan, Professor and Head of the Department of Computer Science and Engineering at Daffodil International University**, for his helpful collaboration and encouraging words, both of which contributed to the successful completion of my thesis.

ABSTRACT

Our home Wi-Fi allows computers and a variety of other devices, such as smartphones and PDAs, to connect wirelessly to the internet. Unsecured Wi-Fi makes it easier for hackers to get to your private files and information and also lets people who shouldn't be able to access your internet do so. Traditional security techniques are insufficient to protect the network nodes because of resource constraints. Numerous security solutions have been developed as a result of network security research. Because wireless channels aren't secure, communications are vulnerable to many types of attacks. Wireless network communications are still a complex and important subject. This article discusses recent developments in security needs and services for wireless network communications. In my paper, I'll mention wifi network security, types of wireless security protocols, and types of wifi security devices, and also mention how the user can minimize wifi network risks.

TABLE OF CONTENTS

CONTENTS	PAGE
APPROVAL.....	I
DECLARATION.....	II
ACKNOWLEDGEMENTS.....	III
ABSTRACT.....	IV
CHAPTER 1: INTRODUCTION.....	01-03
1.1 Introduction.....	01
1.2 Motivation.....	02
1.3 Research Questions.....	02
1.4 Expected Outcome.....	03
1.5 Report Layout.....	03
CHAPTER 2: LITERATURE REVIEW.....	04-06
2.1 Introduction.....	04
2.2 Related Works.....	04
2.3 Research Summary.....	06
2.4 Scope of the Problem.....	06
2.5 Challenges.....	06
CHAPTER 3: WiFi SECURITY OVERVIEW AND THREAT FACTORS.....	07-12
3.1 Introduction.....	07
3.2 WiFi Security Issues.....	07

3.2.1 DNS-Cache Poisoning.....	08
3.2.2 IP spoofing.....	08
3.2.3 Piggybacking and Wardriving.....	09
3.2.4 Evil-Twin Attack.....	09
3.3 Wireless Security Protocols.....	10
3.4 WiFi Network Devices.....	12

CHAPTER 4: TESTING AND MINIMIZING RISKS.....13-24

4.1 Why does a user need to secure his/her WiFi network?.....	13
4.2 Check WiFi Network.....	13
4.3 Configuration for Minimizing Risk.....	14
4.3.1 Create a secure password to access your router.....	15
4.3.2 Give WiFi a unique name.....	16
4.3.3 Disable WPS.....	17
4.3.4 Enable Encryption.....	18
4.3.5 Hide WiFi network.....	19
4.3.6 Set a strong password.....	20
4.3.7 Enable MAC filtering.....	21
4.3.8 Reduce the Range of your Wifi Signal.....	23
4.3.9 Update your Router’s Firmware.....	23
4.3.10 WiFi Router Upgrade.....	24
4.3.11 Use a VPN.....	24

CHAPTER 5: RESULTS AND PREDICTION.....25-28

5.1 Setup for the Experiment.....	25
5.2 Result Analysis.....	25
5.3 Result Discussion.....	28

CHAPTER 6: EFFECTS ON SOCIAL, ECOLOGICAL AND SUSTAINABILITY.....30-31

6.1 Effect on Social.....30

6.2 Ecological Effect.....30

6.3 Ethical Aspects.....30

6.4 Sustainability.....31

CHAPTER 7: SUMMARY, CONCLUSION, RECOMMENDATION32-33

7.1 Summary of the Study.....32

7.2 Conclusion.....32

7.3 Recommendations.....33

APPENDIX.....33

REFERENCES.....34

LIST OF FIGURES

FIGURES	PAGE
Figure 3.2.1: DNS-Cache Poisoning.....	08
Figure 3.2.2: IP spoofing.....	09
Figure 3.2.4: Evil-Twin Attack.....	10
Figure 4.2: Some WiFi manufacturer’s default login credentials.....	14
Figure 4.3.1: Password setup.....	15
Figure 4.3.2: Add SSID.....	16
Figure 4.3.3: Disable WPS.....	17
Figure 4.3.4: Enable Encryption.....	18
Figure 4.3.5: Disable SSID Broadcast.....	19
Figure 4.3.6: Setup wireless password.....	20
Figure 4.3.7.1: Wireless MAC Filtering Setup 1.....	21
Figure 4.3.7.2: Wireless MAC Filtering Setup 2.....	22
Figure 4.3.7.3: Wireless MAC Filtering Setup 3.....	22
Figure 4.3.8: Reduce the range of Wifi signal.....	23
Figure 4.3.11: VPN (Virtual Private Network).....	24
Figure 5.2.1: Router Checking.....	25
Figure 5.2.2: Checking before configuration.....	26
Figure 5.2.3: Checking after configuration.....	27
Figure 5.2.4: Router Checker Results.....	28

CHAPTER 1

INTRODUCTION

1.1 Introduction

Many commercial and military applications employ wireless networks to collect event-driven and real-time data. Network deployment renders them susceptible to security risks. Traditional security techniques are insufficient to protect the nodes because of resource constraints. Numerous security solutions have been developed as a result of network security research. Wireless networks have made it possible for a lot of new applications that need packets to be sent from one or more senders to more than one receiver. Because wireless channels aren't secure, communications are vulnerable to many types of attacks. Wireless network communications are still a complex and important subject. This article discusses recent developments in security needs and services for wireless network communications. Nowadays, it's normal to have internet connectivity at home; it's a household requirement. In the recent past, only a small number of people and organizations could connect to the internet because the infrastructure was expensive and very limited. With improved infrastructure emerging over time, a sizable portion of the world's population can now access and incorporate the use of internet in their daily lives. According to Internet World Stats for March 2019, 56.8% of people worldwide have access to the internet [1]. For instance, household awareness of home network security concerns is quite low compared to the enterprise level. Most people don't give the security of their devices or home network much thought as long as they can access the internet [1]. To avoid the compromise of sensitive information, this mentality must be altered. Preventive measures should be taken to address the problem. However, before doing so, users at home should be aware of how home networking functions and what security flaws affect both users at home and connected devices [1].

Attacks on WiFi-enabled public networks have become more prevalent over the past few years. These attacks occur due to widespread smartphone use and heavy WiFi data traffic [2]. Most people use free public wireless networks to do things like send emails, use social media, and do their banking online. They don't think about whether or not these wireless networks are safe or have been used to start cyberattacks. Intrusion Detection Systems are commonly used in networks to detect malicious activity. However, using such a technique in a mobile setting is difficult [2]. There are many public WiFi networks that people can use in places like malls, cafes, and airports, so they can connect to the internet without worrying about the safety of their surroundings [2].

This research article is about figuring out how safe a public Wi-Fi environment is by using mobile devices. First, an introduction is given, along with a literature assessment of the relevant work that has been done. Next, present a problem description that outlines the justification for the research's purpose. Thirdly, the study includes an implementation strategy that introduces steps for setting up and installing an environment that helps detect attacks. Results and comments on testing public wireless networks conclude the research article. Include the conclusion as well as the references that were used.

1.2 Motivation

- Want to know more about Wifi network security.
- Describe wireless protocols.
- Knowledge about cyber attacks

1.3 Research Question

- Why does a user need to secure their wifi network?
- How does a user check whether their network is secure?
- What are the risks to wireless networks?
- What are the risks to a wifi network?

1.4 Expected Outcome

- Describe a few causes behind the demand for home wireless network security.
- Describe the home WiFi network and how it works.
- Evaluate whether home wireless networks are secure or not.
- Identify and categorize particular instances of attacks in wifi networks.
- Describe wireless security protocols.
- Describe home wifi network security devices.
- Configure all necessary steps to protect home WiFi networks from cyber threats.

1.5 Report Layout

This report varied across a total of seven different chapters. Which are capable of extending the understanding of “Wifi Network Security” more briefly.

In the first chapter, we’ll mention the introduction, motivation, research questions, and the expected outcome.

In the second chapter, we'll go over some related works, the types of challenges we encountered, and the research summary.

In the third chapter, we’ll talk about our research WiFi security overview and threat factors

In the fourth chapter, we’ll talk about testing and minimizing risks

In the fifth chapter, we’ll talk about the results that we got, the analysis of the results, and discussion.

In the sixth chapter, we’ll describe its effects on social, ecological, and sustainability.

In the seventh chapter, which is our last chapter, we’ll mention the conclusion and our future works.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The amount of data that is exchanged every day has gone up because of the Internet of Things, network services, and the exponential growth of internet users [3]. As more information is stored and moved online, cybercriminals try to get access to it so they can do things like sell it on the "dark web" or use it for other illegal purposes. There has been a lot of research on the causes and problems of the security and privacy of wireless networks. It has been found that many factors, especially cybercriminals' growing skills and the lack of preparation and efforts to stop them [3], can make the networks unsafe, including the power of technology and how linked the world is. The growth of the Internet has led to a surge in gadgets like computers, cell phones, and other devices. Wireless technology [4] has contributed significantly to the development of communications. Wireless networks are used a lot in the twenty-first century because they are easy to set up, cheap, and can connect to a lot of other networks. But the growing need for wireless networks and the fact that IoT devices can connect to each other without any security have led to a number of security problems [5, 6]. The privacy of sensitive data, such as personal, financial, and medical information, is also a problem. Concerns about privacy and security are related, and many solutions to one or both of these issues have been created.

2.2 Related Work

Kirti Kaushik and Nidhi Sewal say, "To fight the threat of rogue access points in wireless LANs," which is hard to do at the protocol level, a client-agent-based method for finding rogue access points was made [11]. As a result, a centralized RAP was created for organizations whose service areas are too big to be covered manually or consolidated into one place. Additionally, an algorithm was made to find evil-twin access points, which are hard to find using normal methods, so that the evil twin is separated from the good twin to avoid being caught directly [11].

Different communication protocols make wireless networking possible for various devices [10]. Laptops use Wireless Local Area Network (WLAN) technology to connect to wired networks in the home and business, using all network and internet access options. Using the Bluetooth protocol, devices can sync up with other devices or networked computers from a very short distance away. Cellular technology is used for communication by portable devices like smartphones and personal digital assistants [5]. In this text, we have decided to focus on the first kind of wireless technology: wireless local area network (WLAN) technologies.

According to Alya Hannah Ahmad Kamal, Caryn Chuah Yi Yen, Pang Sze Ling, and Fatima-tuz-Zahra, cybercriminals are attempting to access the growing amount of data being stored and transmitted online [3]. The number of unsafe wireless networks around the world has grown because agencies haven't done enough planning and work to stop them. The purpose of this paper is to highlight significant and common security and privacy issues that arise in wireless networks, along with specialized solutions that can help related organizations or the general public understand how significant an impact these challenges can have if everyone took action to mitigate them [12]. Consequently, it is learned through this paper that there are numerous approaches to lessen these difficulties; yet, the lack of implementation of privacy and security solutions is still primarily evident because responsible parties have not implemented these solutions in real-world situations [12]

Ritika Arora, Sharad, Sanjeet Singh, Narendra Kumar, and A. K. Saini [13] researched phishing attacks and prevention techniques. They find out that identifying phishing is crucial since it is getting worse every day. Phishers pick websites that look and read just like authentic ones. We can look at characteristics like data sets, feature extraction, and detection as preventative measures [13].

2.3 Research Summary

This paper's primary objective is to learn about WiFi network security. How can we minimize the risks? I've reviewed some research papers. In those papers, the researchers have mentioned wifi security prevention techniques.

2.4 Scope of the Problem:

I've reviewed some papers and articles. They stated and used various approaches in those papers and articles. But I will mention, "How can we reduce the risks of our wifi networks?" I think my research will help others.

2.5 Challenges:

I know a little bit about WiFi and wireless network security. For my research, I got a chance to learn more about it.

Conducting research on the basis of a certain subject is a very significant thing to do. Six months is an insufficient amount of time to do research on a subject. Maybe I'll attempt to come up with something fresh in a short period of time. However, there aren't many books on this subject. This study has not received much journal attention, and it is highly challenging to sway the public's attitude on the subject. The victims aren't being completely honest about their issues. As a whole, this area of study contains several gaps.

CHAPTER 3

WiFi SECURITY OVERVIEW AND THREAT FACTORS

3.1 Introduction

The wireless internet connection in your house is via your Wi-Fi network. Typically, a wireless router that transmits a signal into the air is used. That signal may be used to establish an internet connection. However, if your network doesn't have a password, any device nearby can pick up the signal and use your internet connection.

Benefits of Wi-Fi Wireless internet access is available. The drawback? Anyone nearby who connects to your unsecured network may be able to view anything you do online, including your private data. Also, the activity could be tied to you if someone uses your network to do something illegal or send spam without your permission.

3.2 WiFi Security Issues

As more people use mobile devices to access the internet and make transactions online, Wi-Fi network users face the danger of being exposed to several cyber hazards.

The importance of Wi-Fi security has been brought to light because many companies now require their employees to work remotely. Home Wi-Fi networks with poor security are vulnerable to infiltration. This weakness might put the safety of commercial networks in danger.

Furthermore, as public Wi-Fi use increases, companies and individual users are becoming more concerned about security. Since these networks are, by definition, "open," they are not secured. The previously disclosed MITM attack and other malicious behavior may easily infect devices connected to public networks [9].

We will discuss several WiFi security issues in this research.

3.2.1 DNS-Cache Poisoning: Also referred to as DNS spoofing, DNS-cache poisoning poses a threat to wireless networks. This strategy entails hacking a network and redirecting network traffic to a computer or server owned by the attacker or to another out-of-network device. Connecting to a malicious copy of a network that they want to access poses a risk to users [9]. Figure 3.2.1 depicts the DNS-Cache Poisoning attack process.

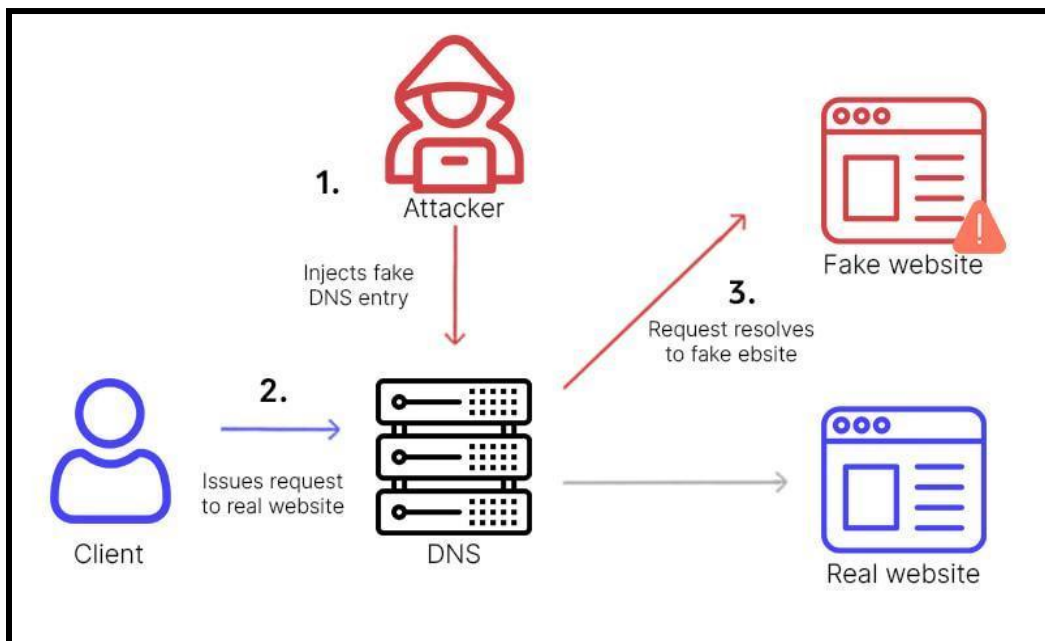


Figure 3.2.1: DNS-Cache Poisoning

3.2.2 IP spoofing: Attackers break into wireless networks using IP spoofing by pretending to be reliable IP addresses. With this strategy, attackers might be able to install malware, launch distributed denial-of-service (DDoS) attacks, or do other evil deeds [9]. The IP spoofing attack process is depicted in Figure 3.2.2.

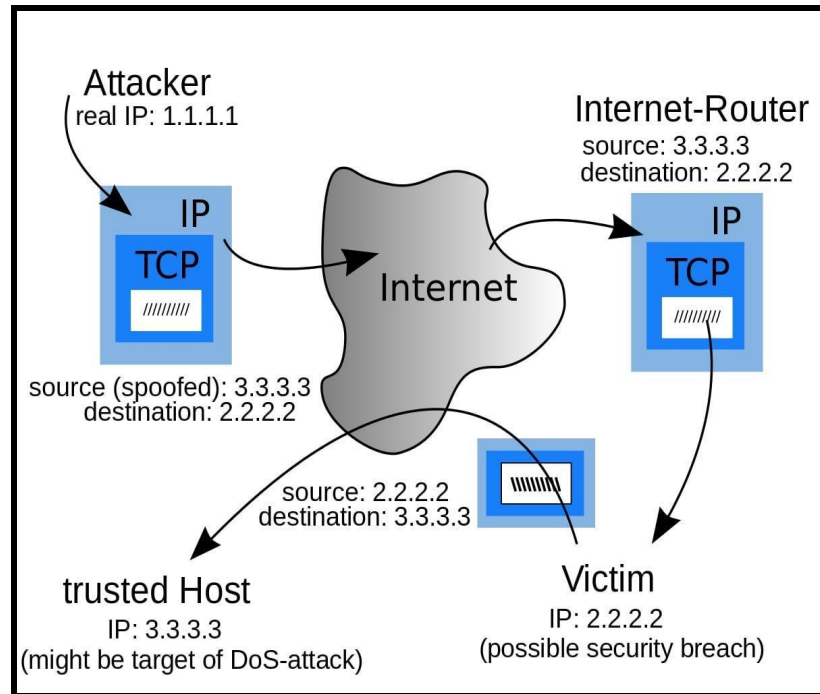


Figure 3.2.2: IP spoofing

3.2.3 Piggybacking and Wardriving: Wardriving is one specific kind of piggybacking. The broadcast range of a WiFi access point allows for the accessibility of internet connections outside of your house, even on the other side of your street. Knowing this, some savvy computer users have made it a pastime to drive across towns and neighborhoods in search of open wireless networks while carrying a wireless computer and sometimes a powerful antenna. This practice is referred to as "wardriving."

3.2.4 Evil-Twin Attack: An attacker finds a public wireless access point and sets up his computer to attack as if it were the evil twin of the access point. Users connect without knowing it by using the attacker's broadcast signal, which is stronger than the signal from the real access point. Since the victim is connected to the internet through the attacker's computer, it is easy for the attacker to use special tools to read any data the victim sends over the internet. This information could contain username and password pairs, credit card numbers, and other sensitive information. Always check the name and password of a

public Wi-Fi hotspot before using it. If you do this, you can be sure that you're connected to a trustworthy access point. The Evil-Twin attack process is depicted in Figure 3.2.4.

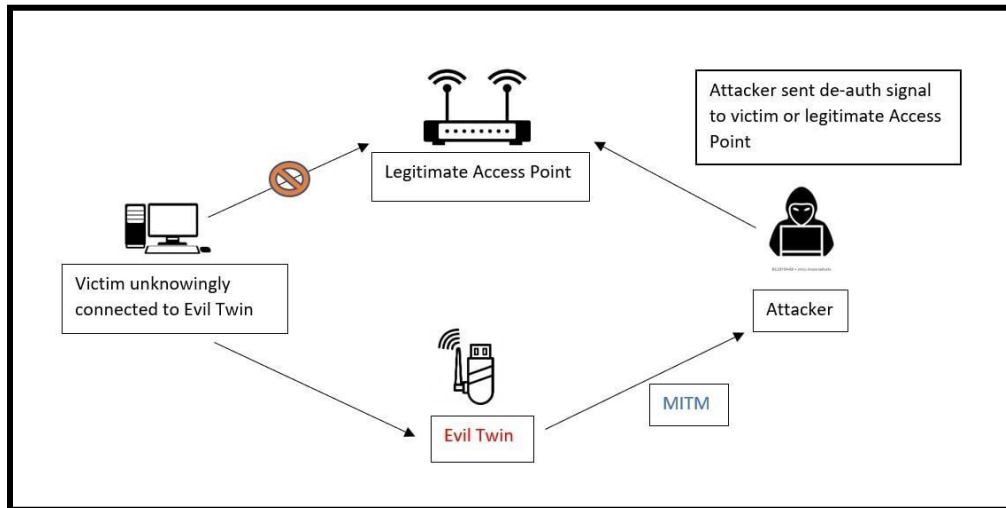


Figure 3.2.4: Evil-Twin Attack

3.3 Wireless Security Protocols

The following list includes the four main wireless security protocols. The Wi-Fi Alliance made these standards. The Wi-Fi Alliance is a group that promotes wireless technology and how it works with other technologies. The group introduced three of the protocols in the late 1990s; they are described in more depth below. The protocols have now been strengthened with the addition of stronger encryption. The Fourth Protocol was made available in 2018.

- **Wired Equivalent Privacy (WEP):** WEP is the most widely used and reputable Wi-Fi security standard. The purpose of the privacy component of IEEE 802.11 was to provide a wireless WLAN with security on par with that of a conventional LAN. In 1999 [10], the Wi-Fi Alliance certified WEP as a security standard. Although initially commended for providing the same security advantages as a wired connection, WEP has been hampered over time by various security problems. And these shortcomings have gotten worse as processing power has expanded. Despite efforts to make WEP safer, it still has security weaknesses. In 2004 [10], the Wi-Fi Alliance formally outlawed WEP.

- **WiFi Protected Access (WPA):** In order to address the rising WEP weaknesses, the WPA wireless security protocol was introduced in 2003. The WPA Wi-Fi protocol is more secure than WEP because it encrypts data with a 256-bit key, a significant improvement over the WEP system's usage of 64-bit and 128-bit keys [10]. The TKIP, another security method used by WPA, dynamically produces a new key for each data packet. TKIP is far more secure than the fixed-key strategy used by WEP. But WPA has certain drawbacks as well. The main WPA component, TKIP, was created to be added to machines with WEP capabilities through firmware updates. As a result, WPA still depends on these frail components [10].
- **WPA 2:** Wi-Fi Protected Access, a wireless security technology, is currently in version 2. The purpose of WPA2 was to secure and safeguard Wi-Fi networks, much like its predecessor. WPA2 restricts access to data sent or received over wireless networks to users who have your network password, much as its predecessor did. WPA2 encryption makes sure that only people who know your network password can see the data sent or received over your wireless network. One benefit of the WPA2 system was that it used Advanced Encryption Technology instead of the more vulnerable TKIP method used in the first WPA protocol. Because AES offers powerful encryption, the US government utilizes it to safeguard sensitive information. Unfortunately, WPA2-enabled access points are vulnerable to assaults, much like WEP's predecessor. To stop this attack vector, deactivate WEP and ensure your router's firmware isn't reliant on it [10].
- **WPA 3:** Using the most recent wireless security standard, WPA3, data is encrypted using the frequent and automated encryption type known as "perfect forward secrecy." It still needs to be commonly used, even though it is more secure than WPA2 [10]. Not all equipment is capable of WPA3 by default, and modifying hardware to make it possible is typically expensive [10].

3.4 Wi-Fi Network Security Devices

- **Active Device:** By thwarting hostile attacks and unwelcome network traffic, a variety of commercially accessible devices can offer network security [9]. One kind is referred to as an "active" device, which consists of hardware set up to prevent extra network traffic. Firewalls, antivirus scanners, and content-filtering devices are a few examples of these Wi-Fi network security devices [9].
- **Preventive Device:** A preventive tool can scan networks to find potential security concerns, such as a wireless intrusion prevention system [9]. Networks can incorporate a WIPS or use separate sensors to overlay it. However, some WIPS merely perform sporadic monitoring, leaving networks sporadically exposed [9].
- **UTM System:** UTM systems combine network security needs, such as firewalls, content filtering, VPNs, antivirus detection, and more. Combining many security measures is made simpler by a UTM system [9]. Doing these tasks at a single location on the network reduces the requirement for point solutions from many providers. Cloud services, virtual appliances, and network hardware appliances can also be UTM devices [9].
- **Passive Device:** Devices for passive Wi-Fi network security may be able to spot and report unauthorized network activities. Other Wi-Fi devices consume more power than passive ones [9]. Since they can only connect with Wi-Fi routers when the routers are actively looking for them, they also provide an additional degree of security [9]. Because of that extra layer, MITM assaults are more challenging. An adversary tries to listen in on two parties' discussions during the MITM attack to "listen in" on their behavior or alter the traffic between them [9].

CHAPTER 4

TESTING AND MINIMIZING RISKS

4.1 Why does a user need to secure his/her WiFi network?

It's conceivable for the network to reach heights of more than 300 feet. To secure the device and safeguard your network, it is essential that you take the appropriate preventative actions [11]. The outdated Wired Equivalent Privacy grade of security is still available on some wifi access points. Make a long, random password to secure your wireless network. Make a special network accessible to visitors. It is strongly advised that you set up a separate network for guests if you frequently let them access your WiFi network due to visitors [11].

4.2 Check WiFi Network

A broadband router sometimes referred to as a "hub" or "wireless router," is a piece of hardware widely used to configure and access household Wi-Fi networks. To check the security settings, you must be connected to your router. The administrator password, the wireless security key, and the encryption technique are the three most crucial parameters. There are several techniques to determine what these settings are, such as

Simple technique:

The first time you connect to your wireless network from any device, you will be asked for the wireless security key. If you haven't changed it previously, it's usually placed somewhere on your wireless router, like the base.

If you are not asked for a key when connecting your device for the first time, your wireless network is not secure. If a key is requested, communication between your device and the wireless network will be encrypted. The finest encryption method on the market could not be used by your wireless network, though.

Advanced technique:

You need to know the IP address of the wireless router as well as the administrator's login and password in order to utilize this approach. Type the router's IP address into the address box after it has been opened (something like 192.168.1.1 or 192.168.1.254). Give the administrator's username and password when requested. Check your router's settings to see whether your connection is already protected and to select a more secure password. Since they are intended to be temporary, the majority of WiFi routers come with usernames like "admin" and passwords like "password" by default. If you don't know the default login information for your router, you can find it on the manufacturer's website, as shown in Figure 4.2.

Router Model	Username	Password
Asus	admin	admin
Belkin	admin	(leave blank)
Cisco	admin, cisco	admin, cisco, or (leave blank)
Linksys	admin	admin
Netgear	admin	password, 1234, or (leave blank)
TP-Link	admin	admin
D-Link	admin	(leave blank)

Figure 4.2: Some WiFi manufacturer's default login credentials

It's not secure if our wifi is still working with the default Username and Password.

4.3 Configuration for Minimizing Risk

Setting up and managing a secure home WiFi network is relatively simple. The steps we take to protect our WiFi network are listed below. While some are more effective than others in discouraging freeloaders and hackers, they are all advantageous in their

particular ways. Even though there is no total defense against hacking attempts, using these tips will make it more difficult for someone to access your network and data.

I'll set up a **TP-Link TL-WR841N** router as an example and demonstrate the settings.

4.3.1 Create a secure password to access your router

- In the address field of your browser, type the router's IP address. You'll be directed to the router's configuration authorization page. On the device and in the user manual, the router's IP address is listed.
- Enter your login information and password on the permission page. You may locate them on the underside of your router if you haven't updated them.
- Go to **System Tools** → **Password** on the router settings page.
- Enter your username and previous password, choose a new one for router access, and then click **Save**. For advice on creating a strong password.

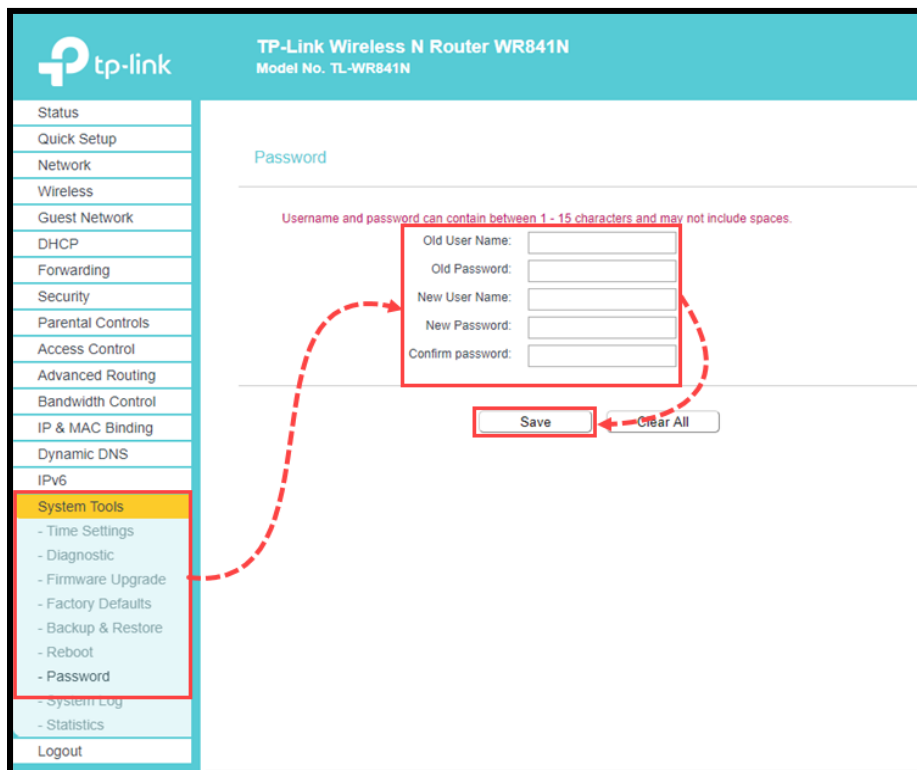


Figure 4.3.1: Password setup

4.3.2 Give WiFi a unique name

- In the address box of your browser, type the router's IP address. You'll be directed to the router's configuration authorization page. On the device's underside and in the user manual, the router's IP address is listed.
- Enter your login information and password on the permission page. You may locate them on the underside of your router if you haven't updated them.
- Go to **Wireless** → **Basic Settings** on the router's configuration page.
- Enter a new name for your wireless network in the **Wireless Network Name** section.

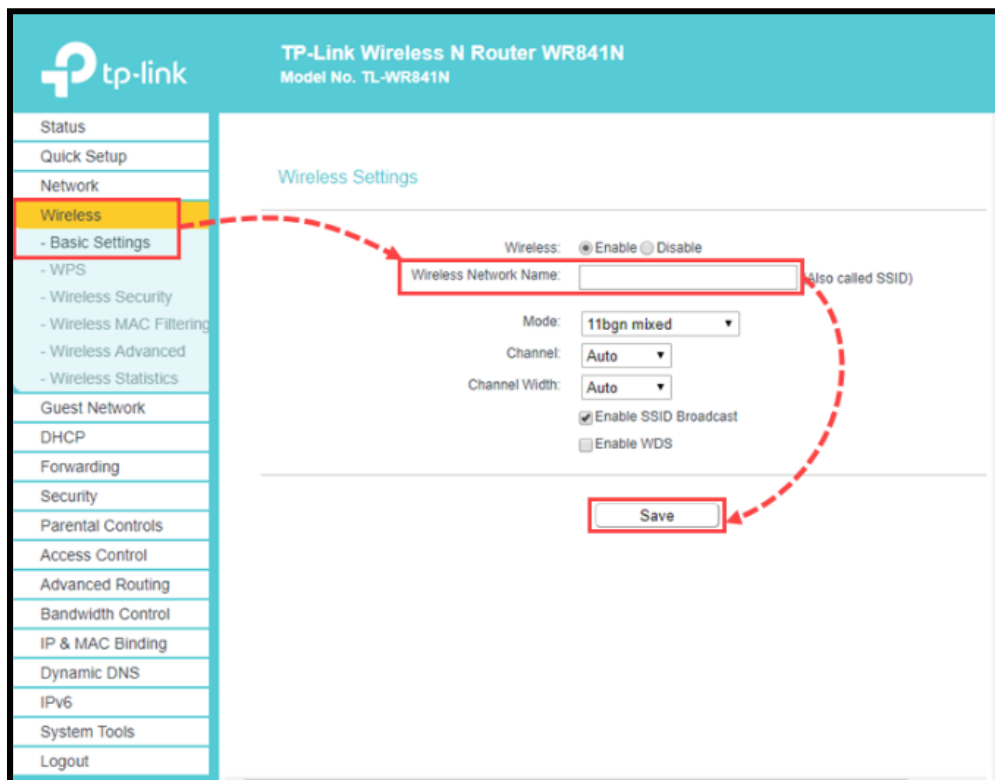


Figure 4.3.2: Add SSID

4.3.3 Disable WPS

WPS technology has made it simpler for devices to connect to Wi-Fi networks. WPS allows you to connect to a router without inputting a password. You should disable WPS in your router's settings, as advised.

- In the address box of your browser, type the router's IP address. You'll be directed to the router's configuration authorization page. On the gadget and in the user manual, the router's IP address is listed.
- Enter your login information and password on the permission page. You may locate them on the underside of your router if you haven't updated them.
- Go to **Wireless** → **WPS** on the router's configuration page.
- Press **Disable**.

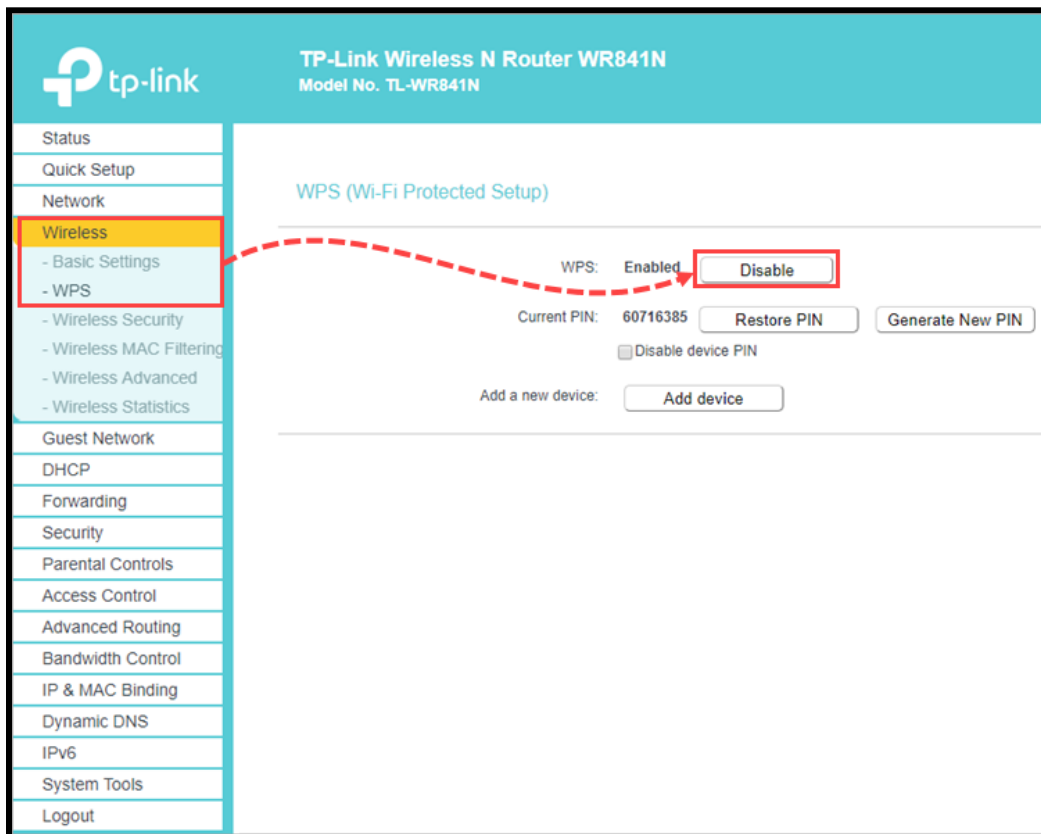


Figure 4.3.3: Disable WPS

4.3.4 Enable Encryption

When you use a network that isn't well protected, criminals may be able to easily steal your information. If you are connected to your home network and you get a notification that it is insecurely encrypted, switch to a more secure encryption type. The three most popular protocols for wireless network encryption are WEP, WPA, and WPA2 (AES/CCMP). The protocols' many degrees of security Since WPA2 is the most reliable, I suggest using it.

- Enter your login information and password on the permission page. You may locate them on the underside of your router if you haven't updated them.
- Go to the **Wireless** → **Wireless Security** option on the router's settings page.
- Then, choose **WPA/WPA2 - Personal**.
- From the drop-down selection for **Authentication Type**, choose **WPA2-PSK**.
- From the drop-down selection for **Encryption**, choose **AES**.
- Press **Save**.

The Wi-Fi network will be equipped with encryption.

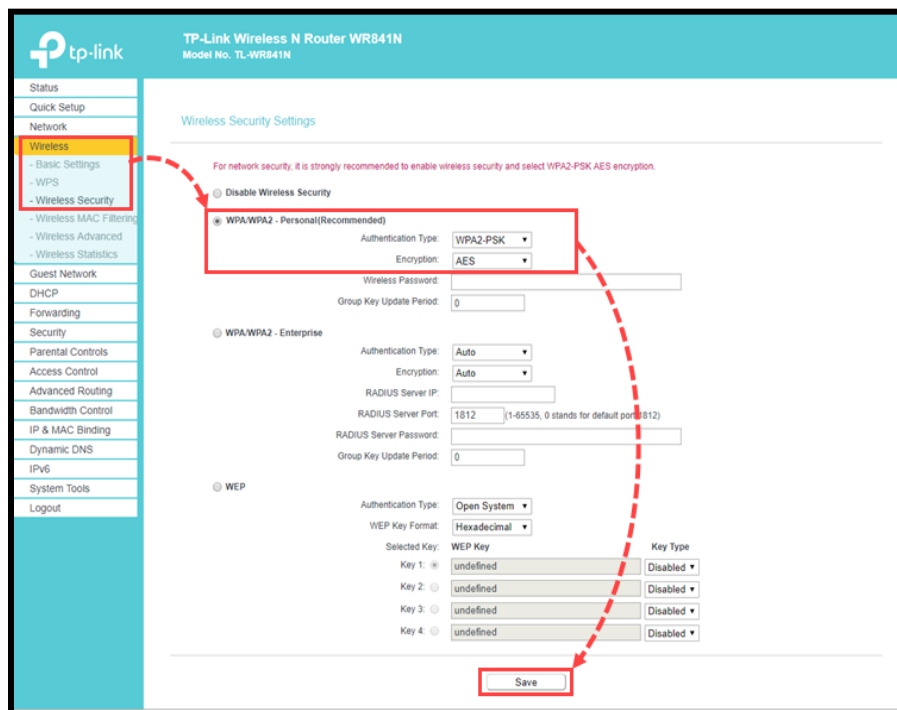


Figure 4.3.4: Enable Encryption

4.3.5 Hide WiFi network

Hide the network name in the router's settings. Your network won't appear in the list of accessible connections any more. It won't be possible to discover it without specialized software.

- Enter your login information and password on the permission page. You may locate them on the bottom of your router if you haven't updated them.
- Go to the router's settings page and choose **Wireless** → **Basic Settings**.
- Remove the check mark from the **Enable SSID Broadcast** box.
- Press **Save**.

Your Wi-Fi network won't be detectable by devices.

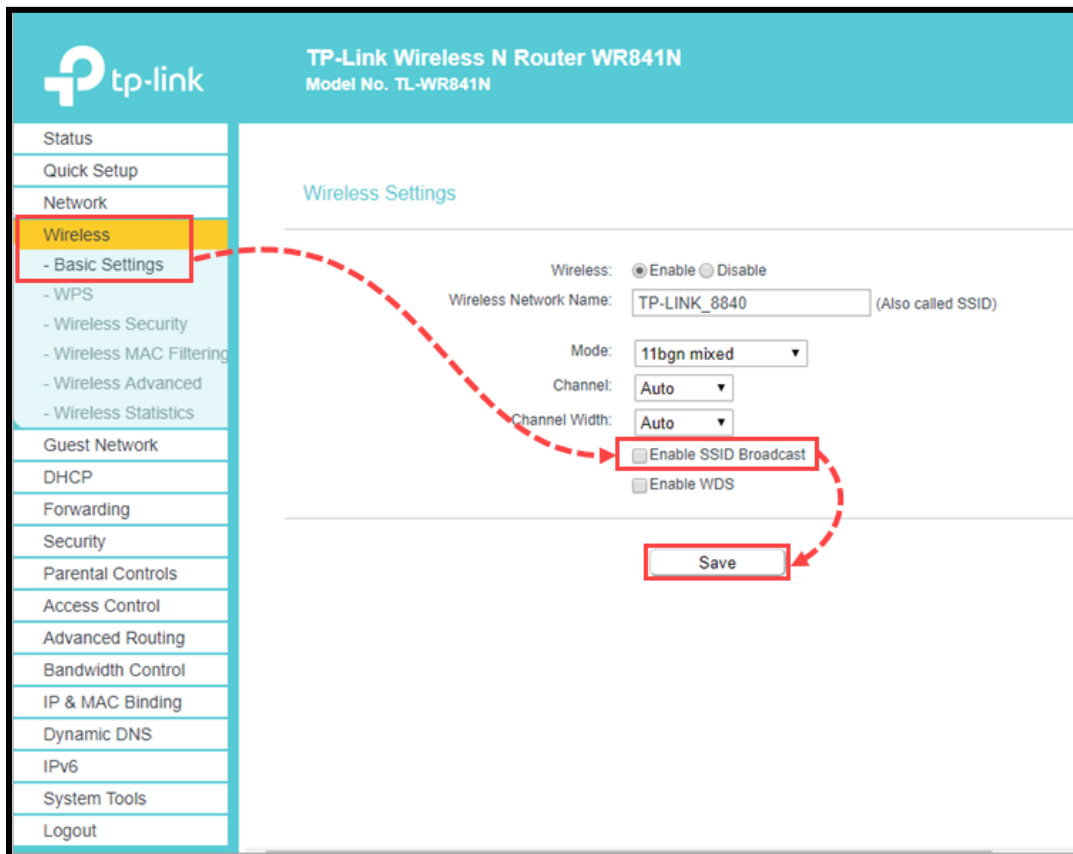


Figure 4.3.5: Disable SSID Broadcast

4.3.6 Set a strong password

Anyone will be able to connect to your home Wi-Fi network without a password. A strong password will stop unauthorized users from accessing your network. For advice on creating a secure password.

- In the address box of your browser, type the router's IP address. You'll be sent to the router's configuration authorization page. On the gadget and in the user manual, the router's IP address is listed.
- Enter your login information and password on the permission page. You may locate them on the bottom of your router if you haven't updated them.
- Go to the **Wireless** → **Wireless Security** option on the router's settings page.
- Then, choose **WPA/WPA2 - Personal**.
- Enter a new WiFi network password in the **Wireless Password** field.
- Press **Save**.

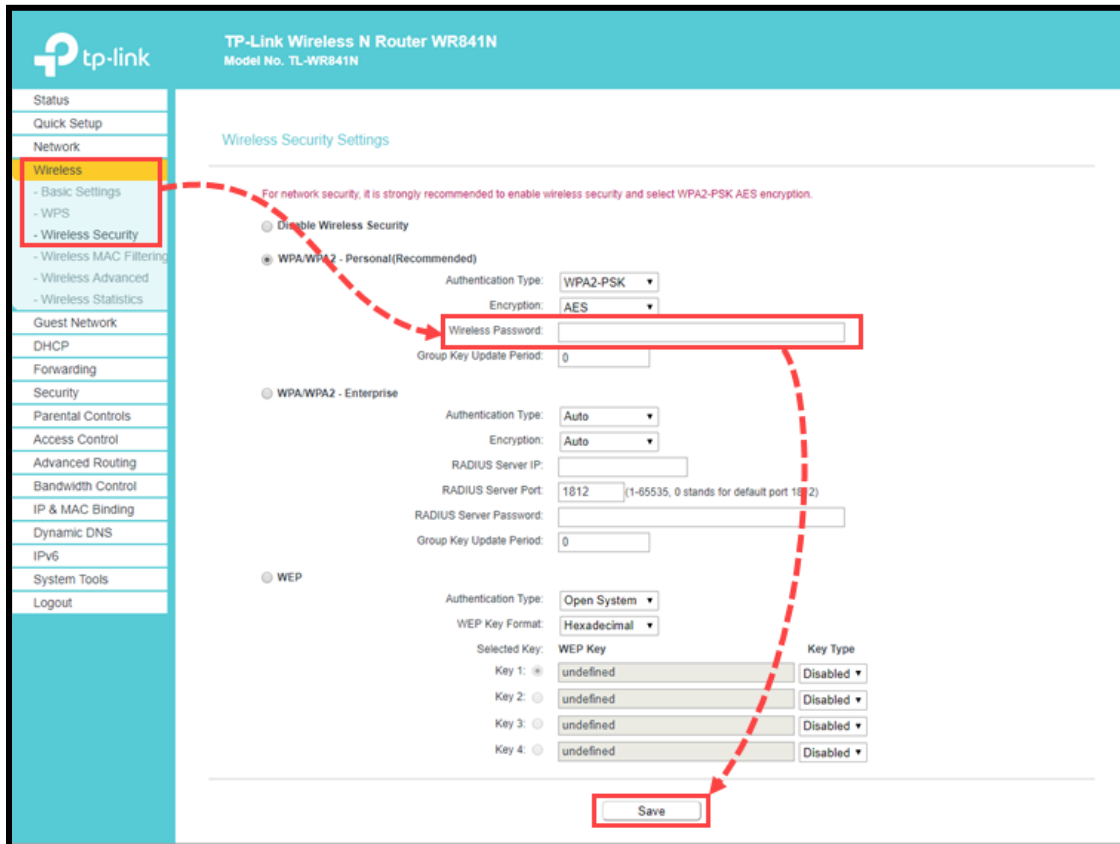


Figure 4.3.6: Setup wireless password

4.3.7 Enable MAC filtering

A MAC address is assigned to any device that has a network interface or network card. Make a list of MAC addresses that are trusted or block access to devices with a certain MAC address.

- In the address box of your browser, type the router's IP address. You'll be sent to the router's configuration authorization page. On the gadget and in the user manual, the router's IP address is listed.
- Enter your login information and password on the permission page. You may locate them on the bottom of your router if you haven't updated them.
- Go to the **Wireless** → **Wireless MAC Filtering** option on the router's settings page.
- Press **Add New**

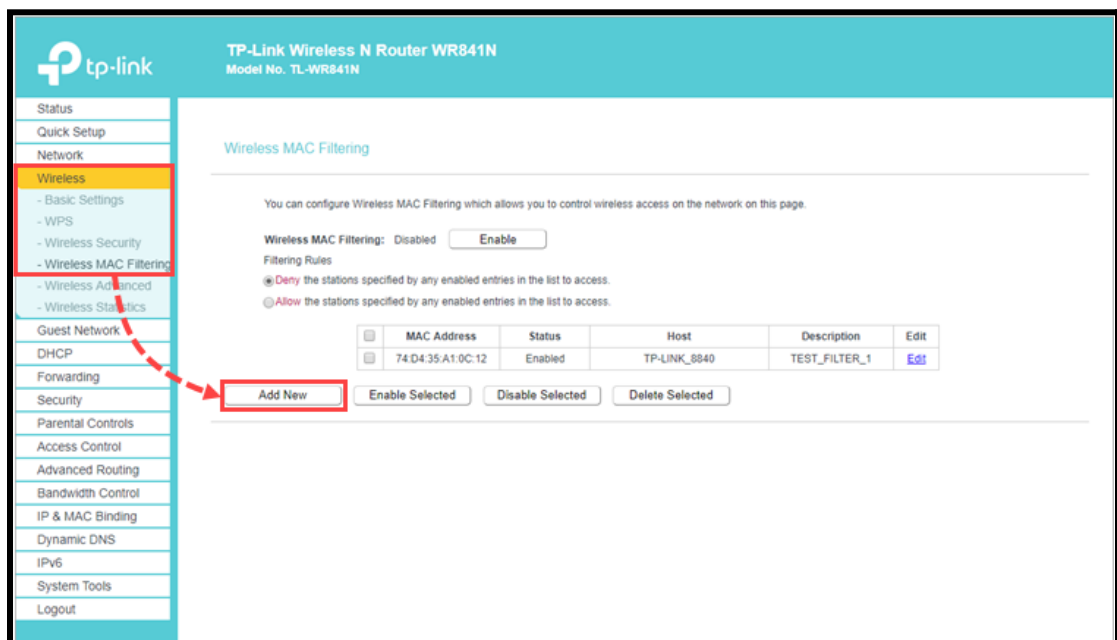


Figure 4.3.7.1: Wireless MAC Filtering Setup 1

- Select the status **Enabled** and provide the device's MAC address and description.
- Press **Save**.

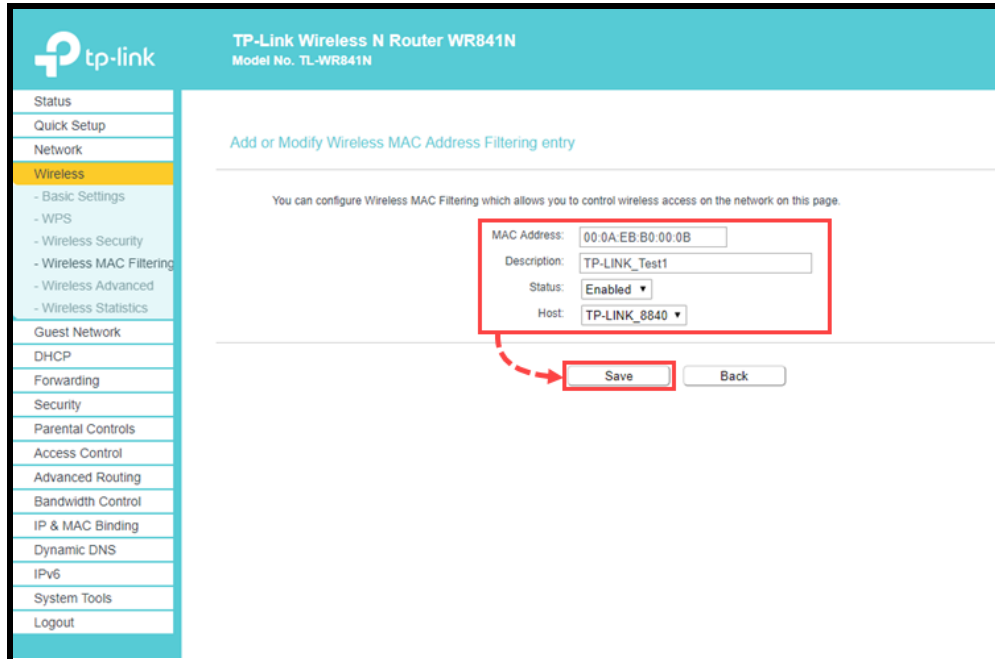


Figure 4.3.7.2: Wireless MAC Filtering Setup 2

- Press **Enable**
- Select **Allow the stations specified by any enabled entries in the list to access.**

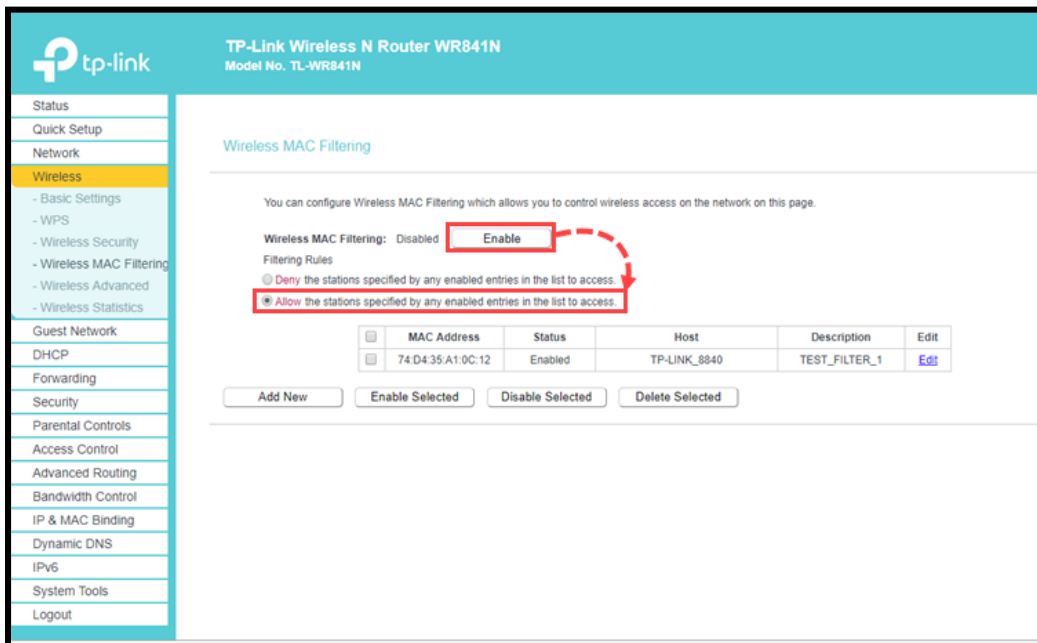


Figure 4.3.7.3: Wireless MAC Filtering Setup 3

The router will only be accessible to the devices whose MAC addresses you have added to the list.

4.3.8 Reduce the Range of your Wifi Signal

- Go to the **Wireless** → **Wireless Advanced** option on the router's settings page.
- Choose a strength, such as **Medium**, from the **Transmit Power** drop-down option.
- Press **Save**.

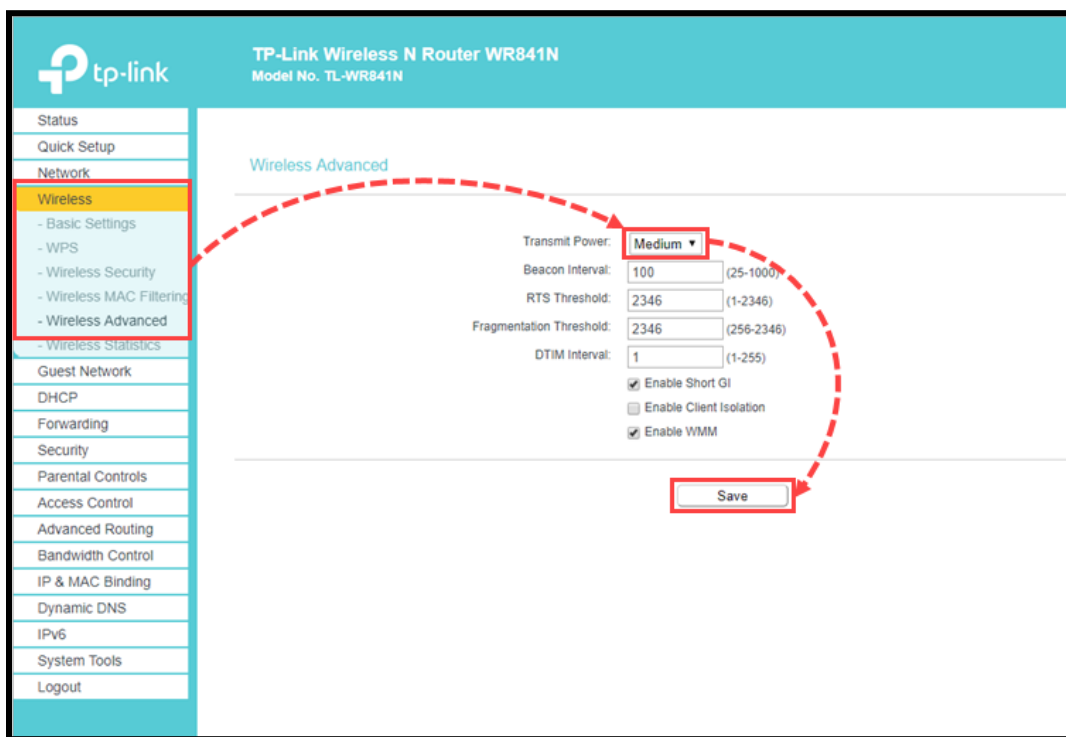


Figure 4.3.8: Reduce the range of Wifi signal

4.3.9 Update your Router's Firmware

Hacking routers is a common practice for cybercriminals. You can update the firmware on your router, which will add fresh security updates, to stay ahead of them. The functionality of your WiFi network may be enhanced by changing the firmware because it functions much like the operating system of your router. Update the firmware on your

router frequently. Updates improve the security of your device and fix bugs and software flaws.

4.3.10 WiFi Router Upgrade

You may want to think about upgrading to a newer model if your router is outdated or if you continue to use the router that your ISP provides. Make sure the router you choose supports WiFi 5 or WiFi 6, has WPA3 encryption, and has at least two WiFi bands when shopping for a new one.

4.3.11 Use a VPN

With a VPN (virtual private network), your private WiFi network is spread across a public network, like the internet. More specifically, a VPN hides your IP address and encrypts your internet traffic by sending it through a remote server. This makes it impossible for anyone to see the data you send or receive online.

You may utilize a VPN service by installing an application or adding an extension to your web browser, whether it is free or premium. However, many routers now have VPNs, so you can easily switch them on to enjoy the majority of the same advantages.

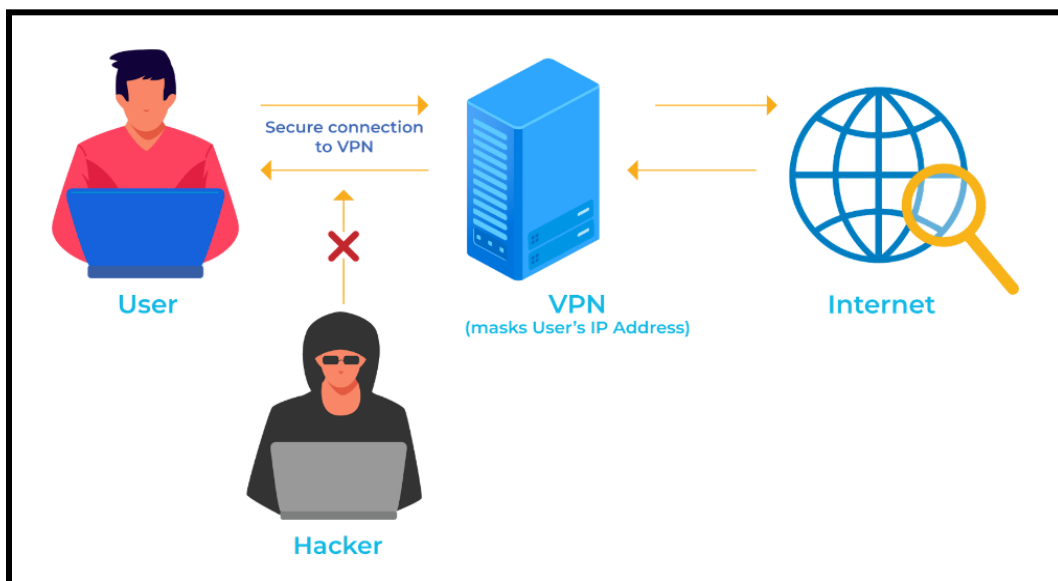


Figure 4.3.11: VPN (Virtual Private Network)

CHAPTER 5

RESULTS AND PREDICTION

5.1 Setup for the Experiment

I use the **F-Secure** router checker to attempt to get a conclusion based on my study. **F-Secure Router Checker** offers a free DNS hijacking test. Hackers that obtain access to your network may spy on you, direct you to fraudulent websites and banks, and even present you with suspicious adverts. We call it DNS hijacking. **F-Secure Router Checker** is risk-free and fast to use.

5.2 Result Analysis

I started by visiting the **F-Secure Online Router Checker** website, selecting the **Router Checker** option under the **Free tools** area, and then clicking the **check your router** button. Figure 5.2.1, which is below, depicts the whole scene.

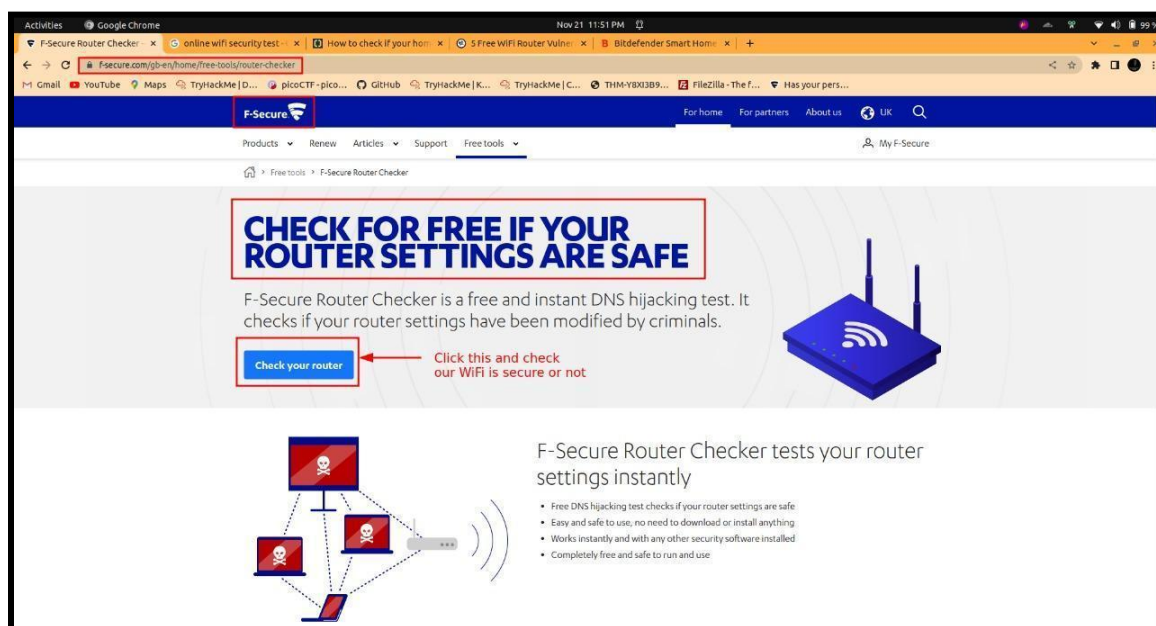


Figure 5.2.1: Router checking

Before security configuration, the security status received from the F-Secure Online Router Checker is shown in Figure 5.2.2 below.

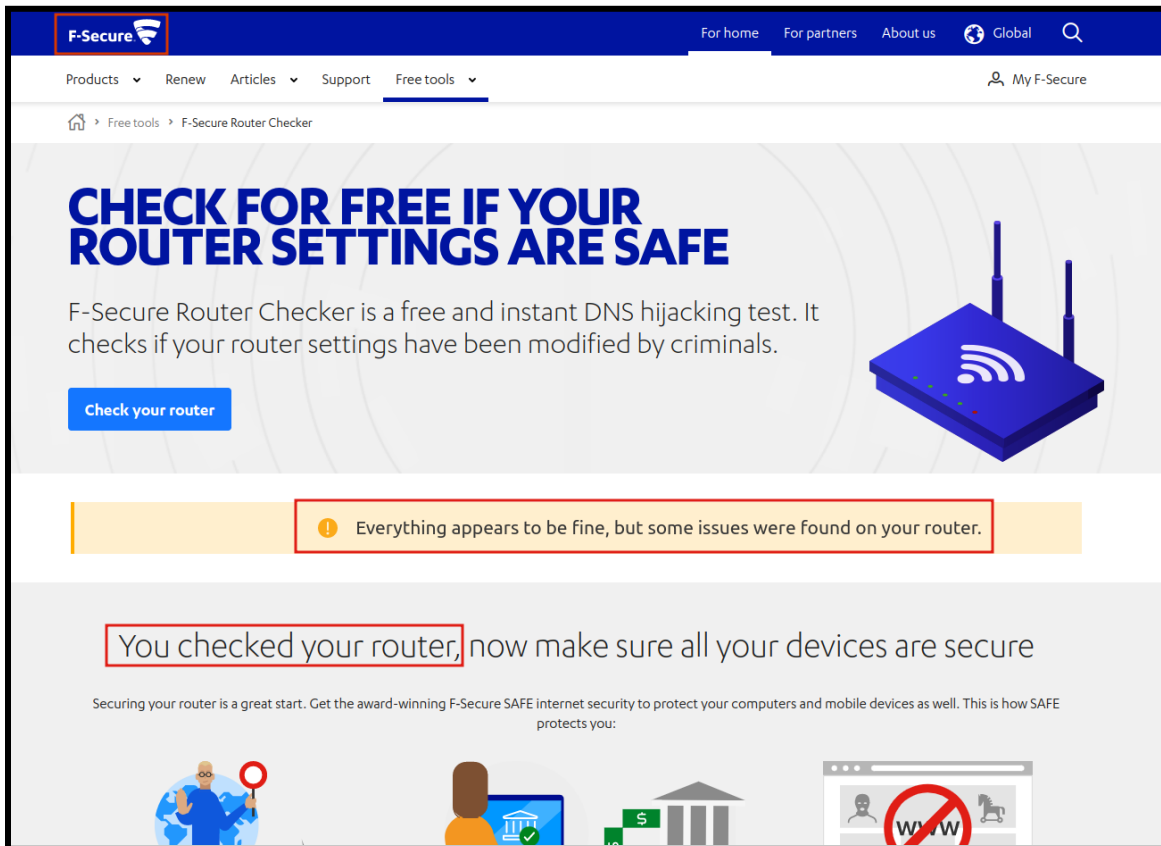


Figure 5.2.2: Checking before configuration

After security configuration, the security status received from the F-Secure Online Router Checker is shown in Figure 5.2.3 below.

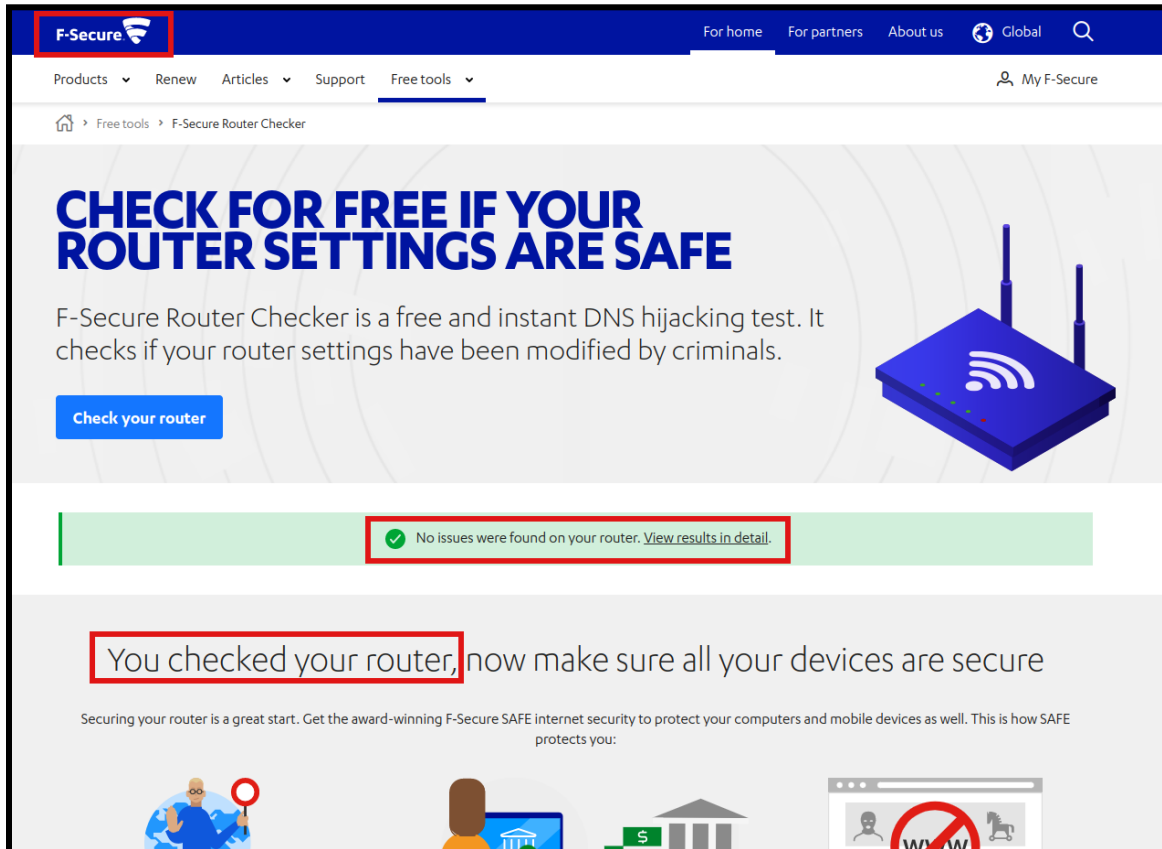


Figure 5.2.3: Checking after configuration

After getting the security status from the F-Secure Online Router Checker web page and clicking on "View results in detail," the Router Checker results will come forward. The entire process is shown in Figure 5.2.3 below.

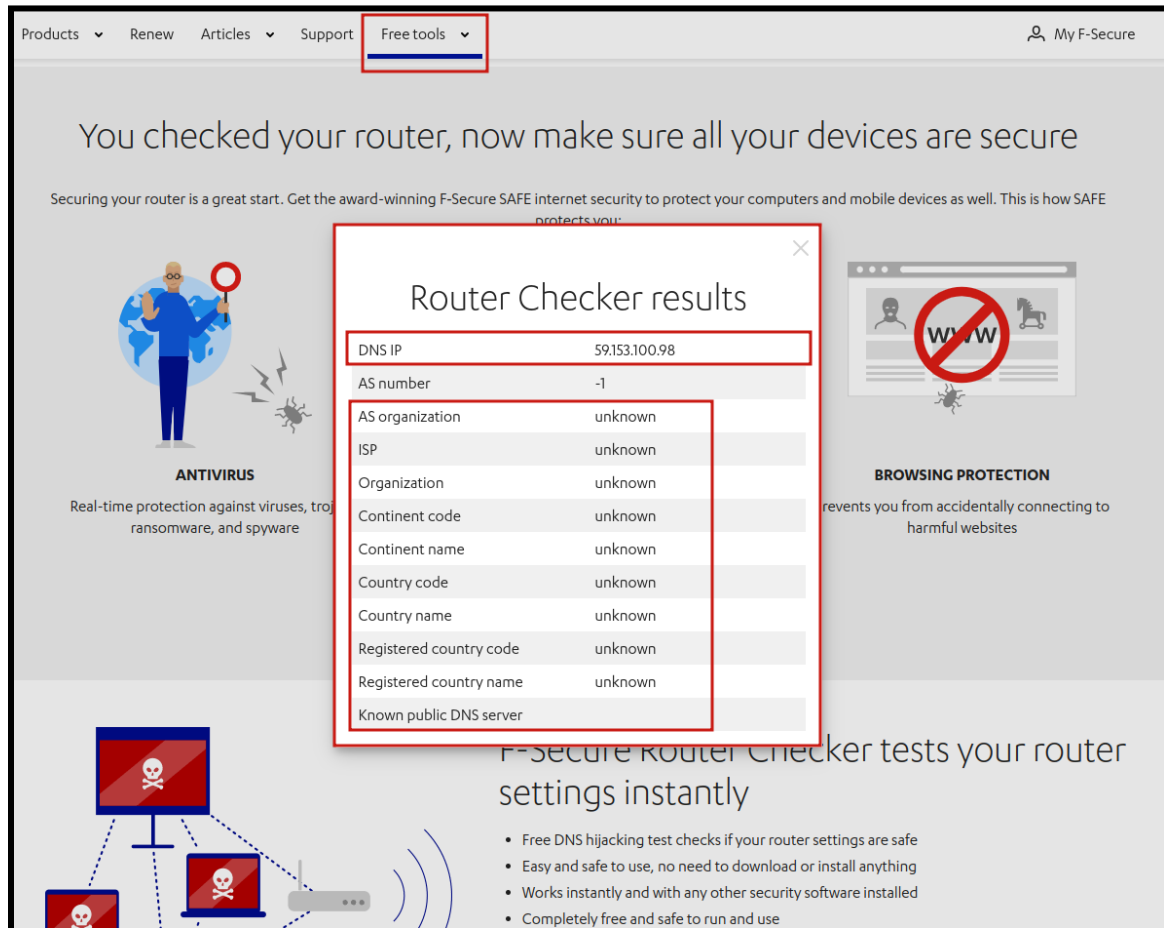


Figure 5.2.4: Router Checker Results

5.3 Result Discussion

Before and after configuring the above security settings on my home's **TP-Link TL-WR841N WiFi router (4.3 Configuration for Minimizing Risk)**, I use F-Secure, a well-known and safe router security checker, to ensure the router's security. Which has already been given in the above-mentioned **5.2 Result Analysis**.

Before configuring security settings on my home's **TP-Link TL-WR841N WiFi router**, the security status received from the **F-Secure Online Router Checker** is **“Everything appears to be fine, but some issues were found on your router”** which is shown in above **Figure 5.2.2**. After configuring security settings on my home's **TP-Link TL-WR841N WiFi router**, I received another security status from the **F-Secure Online Router Checker** which is **“No issues were found on your router. View results in details”** which is shown in above **Figure 5.2.3**. After checking the WiFi router's security with **F-Secure**, they provide a result when I click **View results in details** option. Which is an important part of my research. Through this part, I can evaluate how successful my research has been. If you review the **"Router Checker results"** field in **Figure 5.2.4** attached above, it can be seen that some important information about the WiFi network used at my home, such as **ISP information, Continent code, Country code, Country name, and public DNS server**, is not showing this information. I've already learned from other research papers and cyber security websites that a hacker needs this type of information to attack any home WiFi network. So I think my research has been very worthwhile. Also, through this study, I got to know a lot of new information about cyber security, which will be useful in my later life.

CHAPTER 6

Effects on Social, Ecological and Sustainability

6.1 Effect on Social

The words we read on a daily basis on different internet platforms in the digital world could be connected to every human emotion. In this situation, it is crucial that these platforms have a system in place to separate pre-programmed aggression from actual emotions. This is the reason I've chosen to concentrate on one of the most intriguing genres ever. We may anticipate that by doing this, we will usher in a more distinct and varied digital era.

6.2 Ecological Effect

Due to the complexity of the network system of openness, sharing of resources, linking the variety, the uneven distribution of the terminal, network agnostic, and other barriers, computer networks continue to exhibit their distinctive benefits. The biggest issue is security, which is one of the numerous issues brought on by the network. Unauthorized access, user impersonation, data integrity destruction, system uptime interference, viruses, malicious attacks, wiretapping, and other safety issues that arise in highly open computer network environments cause significant harm. Everybody thinks it is a normal issue, but it is not. So that's why I decided to work on it.

6.3 Ethical Aspects

The internet's media outlets have now become accessible to people of all ages. So, the user limitations no longer work because there aren't enough security measures to tell the difference between moral and social points of view. One must be able to understand the big picture of what a platform is trying to say. In many circumstances, this has been shown to be harmful to people's moral ideals.

6.4 Sustainability

- There are over 2.3 billion active internet-based life clients worldwide.
- At least two internet-based life cycles are present in 91 percent of large business brands.
- It will be a helping hand for researchers.
- Able to gain more knowledge about wifi network security.
- People will be more conscious about their home wifi security.

CHAPTER 7

SUMMARY, CONCLUSION, RECOMMENDATION

7.1 Summary of the Study

Cyberattacks on homes and businesses are happening more and more often every day. To stop attacks, proper cybersecurity measures need to be put in place. There are a variety of techniques to safeguard your Wi-Fi network, according to the paper's author. Some of them include modifying the wireless network's default login details, employing passwords to safeguard your network, and updating the login information for frequent network users. All of these measures will make it more difficult for someone to access your network and use it without your consent.

The goal of this study was to reduce the risks to the security of the wifi network and to better understand wireless networks. This topic has been given an overview in order to achieve this.

7.2 Conclusion

Authors discovered that wireless network security and privacy issues are constantly on the rise but are being overlooked as we move closer to an era of constantly evolving technology, particularly in these unpredictable times when privacy and security of devices and networks are more desired than ever. Cyber Attackers are getting smarter and more persistent, so we think that actions and efforts need to be taken and kept up. Because of the associated organization's failure to protect wireless network security and privacy, these cybercriminals are bombarding and instilling fear in the uninformed public. They are growing stronger and know no fear. Because of enterprises' lack of determination and the general public's ignorance of these pressing issues, it has been discovered that there are still a lot of privacy and security issues in the cyber world. Also, hackers are getting better at what they do, which makes it harder for cybersecurity operations to keep a strong privacy and security system in place.

7.3 Recommendations

- It will be a contribution.
- More easier.
- More flexible.
- User-friendly.

APPENDIX

IP = Internet Protocol

WIPS = Wireless Intrusion Prevention System.

MITM = Man in the middle.

TKP = Temporal keys Integrity Protocols.

WPA = Wifi Protected Access.

WEP = Wired Equivalent Privacy

WPS = Wi-Fi Protected Setup

SSID = Service Set Identifier

MAC = Media Access Control

ISP = Internet service provider

IOT = Internet of things

VPN = Virtual private network

DNS = Domain Name System

REFERENCES

[1]Z. Zainuddin, "Home Network Security," (PDF) *Home Network Security | Zaini Zainuddin - Academia.edu*. [Online].

Available: https://www.academia.edu/40142888/Home_Network_Security. [Accessed: Dec. 19, 2022]

[2]A. Mohamed, "Cookies, Privacy, and Cybersecurity," *Medium*, Jun. 17, 2020. [Online]. Available: <https://medium.com/@azimmohamed2014/cookies-privacy-and-cybersecurity-41c2fc1799b8>.

[Accessed: Dec. 19, 2022]

[3]A. H. Ahmad Kamal, C. C. Yi Yen, P. S. Ling, and F. -tuz-Zahra, "Security and Privacy Issues in Wireless Networks and Mitigation Methods," Sep. 2020, doi: 10.20944/preprints202009.0110.v1. [Online].

Available: <http://dx.doi.org/10.20944/preprints202009.0110.v1>

[4]S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain, and M. Humayun, "Performance Enhancement in Wireless Body Area Networks with Secure Communication," *Wireless Personal Communications*, vol. 116, no. 1, pp. 1–22, Aug. 2020, doi: 10.1007/s11277-020-07702-7. [Online].

Available: <http://dx.doi.org/10.1007/s11277-020-07702-7>

[5]K. R. Rao, "Wireless Communication Security and Privacy issues and Challenges," *Wireless Communication Security and Privacy issues and Challenges | Journal of Computer Science IJCSIS - Academia.edu* [Online].

Available:https://www.academia.edu/34148630/Wireless_Communication_Security_and_Privacy_issues_and_Challenges

[6]N. F. Azhar, Q. J. Ngoo, T. H. Kim, K. Dozono, and F. tuz Zahra, "Security and Privacy Issues in Wireless Networks," Aug. 2020, doi: 10.20944/preprints202008.0523.v1. [Online].

Available: <http://dx.doi.org/10.20944/preprints202008.0523.v1>

[7]"What Is Wi-Fi Security?," *Cisco*. [Online].

Available: <https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html>. [Accessed: Dec. 19, 2022]

[8]"How Vulnerable Is Your Wireless Network? | Anderson Technologies," *Anderson Technologies*, Jul. 19, 2016. [Online]. Available: <https://andersontech.com/wireless-security-vulnerable-network/>.

[Accessed: Dec. 19, 2022]

- [9]J. Ciarlone, “Why Keeping Your WiFi Network Secure Is Important,” *Why Keeping Your WiFi Network Secure Is Important*. [Online]. Available: <https://info.hummingbirdnetworks.com/blog/bid/303317/why-keeping-your-wifi-network-secure-is-important>. [Accessed: Dec. 19, 2022]
- [10]“Wi-Fi Security: WEP vs WPA or WPA2,” *Wi-Fi Security: WEP vs WPA or WPA2* | Avast, Jul. 01, 2022. [Online]. Available: <https://www.avast.com/c-wep-vs-wpa-or-wpa2>. [Accessed: Dec. 19, 2022]
- [11]N. S. Kirti Kaushik, “A Review Paper on Security of Wireless Network,” *A Review Paper on Security of Wireless Network | International Journal on Future Revolution in Computer Science & Communication Engineering*, May 31, 2018. [Online]. Available: <https://www.ijfrcsce.org/index.php/ijfrcsce/article/view/1660>. [Accessed: Dec. 19, 2022]
- [12]V. Singh, K. Bhatia, and S. K. Pandey, “Revisiting Cloud Security Threats Man-in-the-Middle Attack,” *International Journal of Computer Sciences and Engineering*, vol. 7, no. 2, pp. 342–348, Feb. 2019, doi: 10.26438/ijcse/v7i2.342348. [Online]. Available: <http://dx.doi.org/10.26438/ijcse/v7i2.342348>
- [13]Ritik Arora, Sharad, Sanjeet Singh, Narendra Kumar, A. K. Saini, “Phishing Attacks Prevention and Detection Techniques”, *J Arch.Egyptol*, vol. 17, no. 9, pp. 8007 - 8027, Dec. 2020.
- [14]“National Cyber Awareness System,” *Securing Wireless Networks* | CISA. [Online]. Available: <https://www.cisa.gov/uscert/ncas/tips/ST05-003>. [Accessed: Dec. 19, 2022]
- [15]T. Plug, “11 Ways Secure Your WiFi Network - The Plug - HelloTech,” *The Plug - HelloTech*, Sep. 14, 2022. [Online]. Available: <https://www.hellotech.com/blog/how-to-secure-wifi>. [Accessed: Dec. 20, 2022]

Prevention Of Cyber Attacks On Home WiFi Network

ORIGINALITY REPORT

15%	12%	2%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	4%
2	support.kaspersky.com Internet Source	2%
3	www.hellotech.com Internet Source	1%
4	Submitted to Daffodil International University Student Paper	1%
5	www.preprints.org Internet Source	1%
6	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	1%
7	Submitted to The Manchester College Student Paper	1%
8	Submitted to University of Derby Student Paper	1%
9	Submitted to Victorian Institute of Technology Student Paper	<1%