International Journal of Scientific Research and Engineering Development-– Volume X Issue X, Year

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

"During COVID-19, Improving Wireless Network Network Security and Privacy Issues"

ANISHA S. BHOR
Student, Department of Computer Engineering, SPCOE, Otur
anishabhor2000@gmail.com

MONIKA D. ROKADE
Guide, Assistant Professor, SPCOE, Otur
Monikarokade4@gmail.com

----------**********----------

Abstract:

During the COVID-19 outbreak, many organisations that were once intermediate users were victims of wireless network security breaches, which had a significant impact on their businesses and privacy data. This study examines typical wireless network attacks as well as reported security breaches during the epidemic. The study surveyed 56 users to determine their relevant basic information resistance to wireless network attacks. According to the results of the survey, the majority of wireless networks are vulnerable to cyber-attacks. During the epidemic, phishing emails with sensitive information, DoS (denial of service), and social engineering occur, while the majority of respondents do nothing to challenge or search online for a solution to problems. As a result, this study suggests a few simple and cost-effective solutions to increase knowledge among technical and basic users in order to improve their security and privacy concerns when using wireless networks.

KEYWORDS
Wireless network, Internet security, COVID-19, cyber-attack, privacy, and security solution are all terms that can be used to describe a security solution.

----------**********----------

I. INTRODUCTION

COVID-19 is rapidly spreading throughout the world. The outbreak began in December 2019, and Saudi Arabia began dealing with it in March 2020, forcing organisations to adapt and operate remotely, with only 38% of those organisations having a cybersecurity policy in place for you to use. This abrupt change in long-distance performance raises external risks to organisational assets, as employees must use their devices to access their accounts, putting organisational data at risk [1]. During the COVID-19 epidemic, the study conducted a comprehensive study on the level of knowledge and technical challenges faced by these users who switched to remote services. The study's findings are detailed in this study, as are proposed solutions to improve wireless network user security and privacy.

II ORIGIN

Computer equipment such as laptops, cell phones, and desktop computers, Base-Channels that act as a gateway in the middle wireless and wireless networks to transmit signals, and Wireless infrastructure that connects wireless clients to end systems that use a central device as an access point, base channels, and distribution systems are frequently components of wireless network structures. There are a variety of other types of wireless networks; Wireless Area Networks (WLAN) enable in-site users to connect to the Internet (for

 ©IJSRED: All Rights are Reserved

example, universities, schools, and hospitals), Wireless Area Networks (WPAN) enable personal devices of users to connect internally about 30 feet, Metropolitan Wireless Area Networks (WMAN) enable networks within a metropolitan area similar areas between buildings in one city, and Wireless Wide Area Networks (WWAN) enable more than one city to connect. Because wireless networks are an easy target for internet attacks due to the complexity of attackers and advanced tools to support them, some of the typical COVID-19 attacks are listed below [3]: Ransomware is a type of malware that defrauds victims until they pay the amount determined by the attacker. Phishing Email: When a victim discovers fraud, the attacker sends a hidden email in an attempt to obtain personal information.

Email, Malspam: Malware is contained in bulk emails. Footprint: The collection of information on organisations that is at risk of being broken. As threats to wireless networks remain high, appropriate countermeasures must be used to minimise attacks as much as possible.

III. TESTING OUTCOMES

During COVID-19, an online questionnaire will be used to identify user implications in wireless network-related attacks. I had 56 random samples of both tech-based users and non-technicians as targets. The survey asks a series of questions about how to use online. We asked the users we directed if they experienced any type of cyber attack during an epidemic (time of solitary confinement), as well as what types of attacks / threats they encountered and how they dealt with them. Give us a list of common wireless-related attacks from which to choose:

• You couldn't access the website you needed; the icon was always down

• You were buying something online and suddenly the current page was redirected to another page

• Someone from TeleCom / STC offers you to raise your money Wi-Fi is available for free.

• You received a phone call informing you that you had won $1,000 and sharing your bank account information;

• You purchased something online and the website asked you to provide sensitive information;

• Notice someone in your neighbourhood driving a car with strange horns and using a public ID, username, and password.

The study's findings are as follows: most people (66.7 percent) face a criminal attack for stealing sensitive information because "someone called to tell you that you won 1000 $ and share your bank details," (42.9 percent) people face a DoS attack because "you couldn't reach the website you need; sitting low," and (33.3 percent) of the population faces a social engineering attack. 'You buy something online, and the website requests sympathy information such as your Public ID, username, and password.'

We also asked questions to see how people were losing or dealing with the attacks they faced, when the majority of you (62.5 percent) said, "They did nothing" while they were being attacked, because people cannot easily distinguish e-mails from phishing scams, malware websites, social media engineering hypocritical tricks, and so on.

IV. AWARENESS PICTURES IMPROVE USER AWARENES

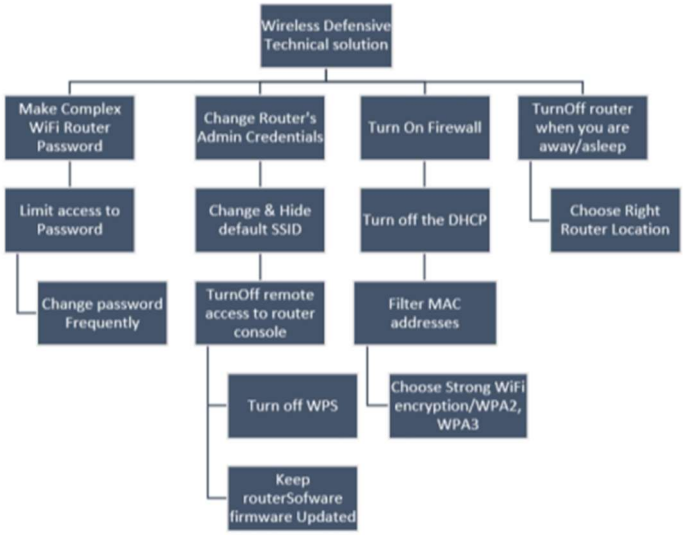
They are worthwhile because wireless network threats are high. Fighting measures should be taken to reduce it attacks, such as adding a complex network password, ensuring proper entry point configuration, switching all network passwords if the device is stolen, and having something else available. Controlled network access via Wifi Secure Access (WPA2 / WPA3), referred to as a wireless network security measure, ensures that all access is protected via HTTPS / SSL, investing in a private professional network that opposes the use of I Weak VPN. Wireless security, when used properly, can help to avoid many attacks; however, because the epidemic broke out suddenly and forced many organisations to work remotely, many were unprepared. Many systems have been reset to correct remote operations, allowing attackers to take advantage of this opportunity. For example, the World Health Organization (WHO) has been the victim of data leaks as well as impersonation of WHO staff in order to solicit donations from the

 ©IJSRED: All Rights are Reserved

general public. WHO, like the majority of organisations, has reviewed their system validation procedure in order to avoid similar situations and develop a better cybersecurity method [4].

In most cases, once a wireless home router is installed and all home devices are connected to the network, we forget about other configurations. However, the internet router is the most dangerous and important device in our homes because it is the gateway to the internet, allowing cyber criminals to sneak in and share confidential and sensitive information. People do not need to be technologists to protect their wireless home network, and they do not need to spend a lot of money to improve security. Only people who must use simple technical solutions in (Fig1) that completely summarises strategies to improve security on wireless home networks [5] [6] should do so.

Figure 1 shows the development of a wireless network.



COVID-19 is still a current epidemic, and despite the fence the technology is already embedded very securely measures, it is especially important to inform users how to deal with these threats in a timely manner without the need for technical experts. The findings of our study suggest that we focus more on moderate users in order to raise their awareness of their own wireless network security and privacy while also preventing and reducing cyber-attacks through subsequent actions (Fig. 2)

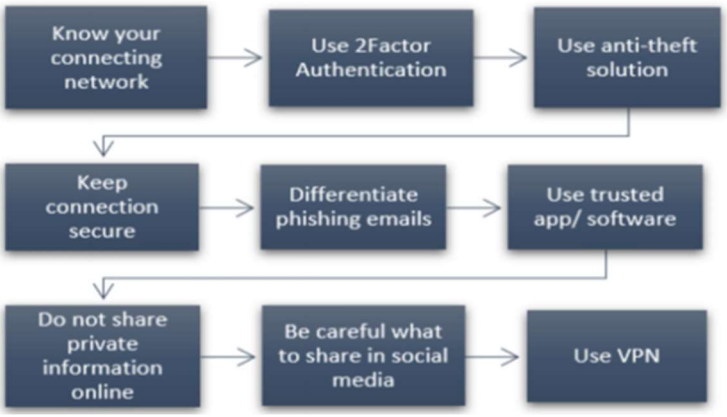


Figure 2: Enhancing User Privacy.

V. CONCLUSION

The current state of the epidemic has revealed whether or not organisations were prepared to operate remotely. As it was a simple goal hijackers, many safety concerns were raised. Applying appropriate safety measures for wireless networks may be costly, but it is critical that every organisation invest heavily in wireless security. COVID-19 cannot be identified because it occurs suddenly. Futuristic situations are the same, and then the attackers who try to interfere but fail will try harder the next time, successful attackers who are caught will learn not to get caught the next time, and finally the robbers attacked, they succeeded, and they were not caught, and they will undoubtedly be as strong as time goes on. Organizations that use expensive professional networks that are private and can protect the entire network are less likely to be targeted by intruders, and the lesson you can learn from this epidemic is that business continuity plans should include this. Combating online security threats and investing in it. Internet security should be improved. Ordinary users should take simple technical and privacy measures to improve the security of their proposed wireless home network.

VI. REFERENCES

1.Pranggono, B., & Arabo, A. (2020). COVID -19 "During COVID-19, Improving Wireless Network Network Security and Privacy Issues"

2.Monika D.Rokade ,Dr.Yogesh kumar Sharma,"Deep and machine learning approaches for

 ©IJSRED: All Rights are Reserved

anomaly-based intrusion detection of imbalanced network traffic." IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719

3. Monika D.Rokade ,Dr.Yogesh kumar Sharma"MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE

4. Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2324 - 2331.

5. Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", **IOSR Journal of Engineering (IOSR JEN),** ISSN (e): 2250-3021, ISSN (p): 2278-8719

6. Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Data Hiding In Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349, Volume : 4, Issue : 5

7. Sunil S.Khatal Dr. Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2340 - 2346.

 ©IJSRED: All Rights are Reserved