International Journal of Multidisciplinary Studies and Innovative Technologies

e-ISSN: 2602-4888
dergipark.org.tr/en/pub/ijmsit
Research Article

2024, 8 (1), 46-51
DOI: 10.36287/ijmsit.8.1.8
Received: July 3, 2024; Accepted: July 22, 2024

# Security Issues of Remote Work Environments and Alternative Solution Approaches

Can Kılıç[1*], İsmail Berk Uzun[2], Abdullah Taha Ardogan[1], Wardah Saleem[1], Arda Sezen[3]

[1*] *Graduate School of Natural and Applied Sciences, Dept. of Software Engineering, Atılım University, Ankara, Türkiye (kilic-can@student.atilim.edu.tr)(ORCID: 0009-0007-4567-3216)*
[2] *Graduate School of Natural and Applied Sciences, Dept. of Computer Engineering, Atılım University, Ankara, Türkiye (uzun.ismailberk@student.atilim.edu.tr)(ORCID: 0009-0002-2260-4326)*
[1] *Graduate School of Natural and Applied Sciences, Dept. of Software Engineering, Atılım University, Ankara, Türkiye (ardogan.abdullahtaha@student.atilim.edu.tr)(ORCID: 0009-0004-7710-4913)*
[1] *Graduate School of Natural and Applied Sciences, Dept. of Software Engineering, Atılım University, Ankara, Türkiye (saleem.wardah@student.atilim.edu.tr)(ORCID: 0009-0006-2145-293X)*
[3] *Dept. of Computer Engineering, Atılım University, Ankara, Türkiye (arda.sezen@atilim.edu.tr)(ORCID: 0000-0002-7615-3623)*

***Abstract –*** Along with the pandemic, the number of remote employees has significantly increased. With this increase, also the cyberthreats related to remote workers greatly increased. So, the main question of how remote working affects cybersecurity tried to be explained by analyzing common threats and mitigations in this study. Throughout the analysis, it is found that two more aspects should be investigated: The threats affecting the remote workers and the mitigations affecting the related threats. To answer these questions sufficiently, well-known cyber-attacks were explained using various studies with countermeasures in the third section. Then, we focused on effective security practices and tools and how to make those practices and tools more effective. To provide sufficient guidance about how to use these mitigation ways for which attack types, a complete guideline is provided for the remote workers. Also, a questionnaire was conducted among some university students to understand the awareness of phishing attacks using wrong URLs and website and email scams from many organizations, and the results show that for the URL part, the accuracy is 84.61%, and for the email scams accuracy is 75.64%.

***Keywords*** *– Remote Work Environment, COVID-19, Cybersecurity, Remote Work Guideline, Awareness for Cyber Threat*

***Citation:*** Kılıç, C. et. Al. (2024). Security Issues of Remote Work Environments and Alternative Solution Approaches. International Journal of Multidisciplinary Studies and Innovative Technologies, 8(1): 46-51.

## 1. INTRODUCTION

In today's world of smart technology, working remotely is becoming more and more prevalent. The phrase "new way of working" describes work practices that enable remote employees to do tasks without needing to be physically present, such as from their homes, coffee shops, or other locations. While this new working mode provides advantages such as flexibility, productivity, and work-life balance, it also introduces substantial security vulnerabilities. However, together with these advantages, people should be aware of various assault types. These attack types include social engineering, phishing, malware, ransomware, man-in-the-middle, evil twin, denial-of-service, cross-site scripting, advanced persistent threats, and zero-day attacks. This paper aims to show the cyber-attack types in remote work environments and the importance of effective security practices and tools against these attacks. The analysis of these assaults and the ways to mitigate them aims to provide a comprehensive understanding of security in remote work environments. In addition to the analysis of assault and mitigate types, this paper also presents two case studies related to only remote work environments to show the real examples of cyber-attacks and how organizations mitigate them. As a last section, a complete guideline is suggested for remote workers to provide useful cyber-attack tips.

## 2. BACKGROUND STUDY

The main purpose of this research is to answer the question of how remote working affects cybersecurity by analyzing common threats and mitigations. During the COVID pandemic, most organizations forced their employees to work from home, coffee, or other locations to ensure no physical presence existed. This situation caused a huge increase in remote workers, and because of that, a surprising user growth in remote communication platforms such as Zoom was observed. Excessive usage of cloud platforms and local and wide area networks to communicate between servers, and employees increased the cyber-threats proportionally. Although it's impossible to eliminate cyber threats completely since they continue to emerge with the rapid progress in technology every second, applying effective mitigations can reduce their impact or probability of occurring and causing significant damage. In the related literature, to show the effects of the pandemic, Rakha stated that the pandemic has increased remote work usage, highlighting the cybersecurity risks that enterprises and policymakers worldwide face. These issues include legal consequences, the need for clear rules, secure remote access, and ongoing cyber threat mitigation training [1]. Khan and Charan explain that the impact of the COVID-19 pandemic on remote labor, including its growing prevalence and long-term survivability. It discusses both the

advantages, such as shorter travel times and cost savings, and the disadvantages, such as security concerns and work-life balance issues. Furthermore, the study identifies frequent security threats connected with remote work and emphasizes the importance of creating routines, specialized workplaces, good communication, and self-care habits to ensure remote work success [2]. To show the importance of awareness, Senapati and Bharathi stated that the study evaluation stresses the lack of cybersecurity knowledge among remote workers, which is attributed to unsafe online habits, company regulations, and teleconferencing system vulnerabilities. During the pandemic, scientific studies and online surveys revealed that individual internet habits and understanding of cybersecurity best practices favorably influence employees' compliance with security standards. However, organizational requirements have less of an impact [3]. As to the usage of mobile devices three studies come forward, Milson and Altan address particular cybersecurity issues about remote work, such as the threat presented by insecure home networks, personal device vulnerabilities, and phishing attempts [4]. Buckley investigates increased cybersecurity risks in remote work during COVID-19, linking them to employee behavior and compliance issues. It detects technological vulnerabilities in personal devices, which are worsened by psychological variables such as unprotected Wi-Fi and bad cyber hygiene practices, as well as organizational restrictions such as restricted access to essential resources. The proposed remedies include adopting rigorous technological restrictions like VPN and MFA and role-specific training sessions delivered by trusted corporate executives [5]. The research of Sandamali examines the impact of mobile devices and new technologies on remote work in the software industry, and it concludes that remote software workers bear a greater burden and are more conscious of the Information Security Policy. The findings emphasize the need for policy implementation improvements and propose recommendations to promote ISP effectiveness, emphasizing private sector Internet service providers and the objective of maximizing remote work efficiency [6]. In addition to these studies, there are many studies that have been researched and used to provide sufficient knowledge about the cyber-attack types like phishing, malware, and man-in-the-middle, and how to mitigate ways against those attacks like using VPN, firewall, and encryption, together with a complete guideline to help remote workers.

## 3.ATTACK TYPES AND COUNTERMEASURES

### *A. Attack Types*

Attack types and their effects on the user have been researched as a first stage, and the research articles found investigated. The comparisons show that the attack types are similar and can be summarized under a few titles. To give an example, Vásquez and González [7] at first took Social Engineering as their focus. In this kind of security threat, breaching is done by manipulating the individuals. So, the strength of this type of attack heavily depends on the physiological capabilities of the attacker. Manipulations can be done in multiple ways: physical, social, technical, and combination. In a physical attack, an attacker actively tries to find the physical location of sensitive data using methods such as dumpster diving. As to the social attack which is the main issue for the remote workers, there is a physiological relation between attacker and victim such as building a relationship, baiting or phishing. The combination of social and technical attack types used to increase the success rate of the attack. While doing these manipulation attacks the attacker is trying to gather information such as usernames and passwords which can be summarized as sensitive data related to the victim. Furthermore, these attacks are able to bypass hardware and software used to prevent attacks. So, the fundamental of getting protection from these attacks is the awareness of users. As it is stated above the research is taking the COVID era in more detail and it is stated by the authors that phishing attacks are the most common attack type.

#### *1. Phishing Attacks*

According to Hong the first stage in a phishing assault is identifying a possible target. The attacker then sends the victim an email directing them to a bogus website where they enter sensitive information, or the attacker installs malware on their system. In the final stage, the cybercriminal can use this sensitive information for personal gain [8].

#### *2. Malware Attacks*

This attack type's main purpose is to threaten a system's integrity, confidentiality, and availability. Additionally, there are multiple types of malware: Adware, which causes pop-up ads, or browser redirection. Downloaders cause the installation of additional things on an infected system. A macro virus is a virus that is embedded in a document and runs and replicates itself into other documents whenever the first document is viewed or edited. Spammer Programs cause you to receive large volumes of unwanted emails. Spyware captures information and sends it to another system via scanning files, monitoring keystrokes, screen data, and so on. Trojan horse viruses can evade security mechanisms by appearing useful while functioning hidden and potentially malicious in the background. Worms are computer programs that may operate independently and spread a fully functional version of themselves to other computers on a network by exploiting software weaknesses. Zombie/bot software is installed on an infected system and activated to launch attacks on other devices [7].

#### *3. Ransomware Attacks*

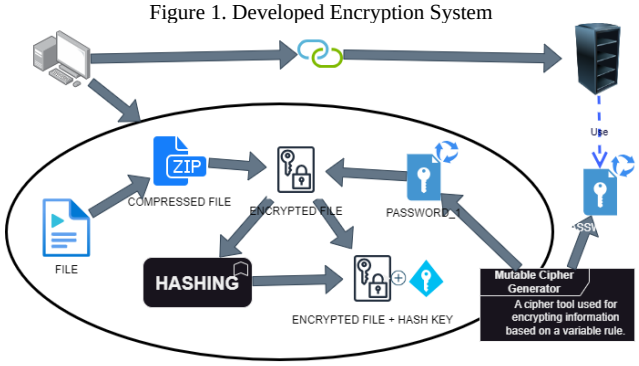
Ransomware is a cyber assault that encrypts a computer's operating system, prohibiting the victim from accessing the computer or a specific file. The attacker then demands a ransom from the victim, which must be paid to acquire a key that allows them to restore access [9].

#### *4. Man-in-the-Middle*

Aliyu et al. stated that the Man in the Middle attack type is one of the most notorious attacks in computer networks. This attack is carried out by a malicious internal user pretending to be the other user on one of the two computers. There are two categories for this attack type. Eavesdropping is passive since the only focus is the passing through information. In Manipulation, the focus is changing the data while masquerading it as the original sender [10].

To explain this attack type in a detailed way, a project explained in Figure 1 below was designed.

Figure 1. Developed Encryption System




In Figure 1, The developed system encrypts data using a pre-implemented cipher, facilitating secure communication between two parties. Furthermore, it guarantees data integrity by transmitting the hash value of the data separately to the destination. The predetermined cipher generates new keys in compliance with specific rules, eliminating the need for mutual notification between the parties. Additionally, the keys derived are identical on both ends.

*5. Evil-Twin*

Evil twin attacks are a serious threat as they can impersonate legitimate Wi-Fi networks to the point of being unrecognizable. Attackers establish these fake networks to deceive users into logging in, which can result in illegal access to user data or the theft of personal information. Hackers can quickly access user data and steal personal information. This poses a substantial risk to individuals who use the same username and password for many accounts, as the hacker can access them all with a single login attempt [11].

*6. Denial-of-Service*

It is observed that this attack type's main purpose is not creating a breach but disrupting the access of users to systems and/or services by exploiting the capacity limit of the system resources. To give an example of this attack type's usage area, it can be said that political attacks on opponents, hacktivism, and financial extortion can be shown. During the pandemic, a type of DoS, DDoS, which is Distributed DoS, is used by attackers using different techniques and tools to attack a specific resource from multiple devices [7].

*7. Cross-Site Scripting (XSS)*

Cross-site scripting (XSS) is a programming problem when user input data is not properly sanitized. The attacker uses this vulnerability to insert unfiltered scripting code into the online application, resulting in account takeover, session or cooking theft, and rerouting to the attacker's website when the parser processes the script [12].

*8. Advanced Persistent Threats*

These are assaults in which attackers acquire unauthorized access to a system and remain unnoticed for a lengthy period in order to collect sensitive information [1].

*9. Zero-Day Attacks*

These attacks use undiscovered flaws in systems or software, making them challenging to identify and stop [1].

*B. Countermeasures*

Especially during the pandemic, Vásquez and González [7] stated that the transition from physical work to remote work gained many paces. However, this pace resulted in non-compliant practices and policies for employees in remote work environments. Additionally, insufficient preparedness and a sudden increase in the wide usage of technology put organizations and their employees in a vulnerable position to cyber threats that are stated above. Evidence of this can be seen in the World Economic Forum Global Risk Report of 2022, stating that in 2020, malware and ransomware increased by more than 350% for both categories [13]. As a result, it is important to study the mitigation of cyber threats and increase the awareness of organizations to eliminate risks.

## 4. EFFECTIVENESS OF SECURITY TOOLS AND PRACTICES

With the advancement of internet communication, cyber threats are spreading out in every area with a network. This spreading caused many different security tools and practices to emerge according to that area's needs. In this section, the main cause of these cyber threats, which is an unsecured connection, is taken into consideration, and how to secure a connection is explained by showing their effects on the connection. We consider four tools and practices: Encryption, Firewall, VPN, and Human Factors, respectively. The following three questions are investigated mainly: What is this tool or practice about? What happens if it is not available? and How can it be more effective?

*A. Encryption*

Encryption protects the original data, known as plaintext, by transforming it into encrypted data, known as ciphertext, using algorithms such as AES, RSA, and Blowfish, as well as a secret key or password. The ciphertext is readable only to the authorized people who know the secret key. Encryption can be applied to any digital data, such as email, and stored data in a disk [5].

When there is no encryption, using insecure protocols like FTP, TELNET, and SNMP while transmitting unencrypted data exposes the data as plaintext, and that vulnerability increases the risk of data breaches. Keeping sensitive data in plaintext can also result in financial losses, regulatory fees, and reputational damage.

According to the literature, there are four main ways to measure or show the effectiveness of encryption: strength, performance, compliance, and testing, respectively.

Encryption strength refers to the difficulty it creates for those attempting to attack. The factors that influence the strength are the algorithm type, the key size, and the implementation details of that encryption. In general, the stronger these factors are, the more secure sensitive data is [14].

Encryption performance refers to how much it affects the victim's network speed, bandwidth, latency, and dependability. The performance is affected by the amount of sensitive data, the availability of hardware and software resources, network topology, and encryption settings. In general, the higher these variables are, the better the user experience and operational efficiency [14].

Encryption compliance refers to the extent to which the encryption meets the industry, sector, or region's legal and regulatory obligations and expectations. The factors

influencing compliance are data type, location, jurisdiction, and encryption standards and policies. In general, greater compliance reduces the likelihood of incurring fines, penalties, lawsuits, and reputational damage [14].

Encryption testing comprises modeling and assessing various possible scenarios and attacks that might compromise data and networks. Many factors impact the testing process, including the kind and scope of testing, the methodology and tools utilized throughout the testing phase, the results, and the reports given. It is reasonable to infer that the more comprehensive the testing, the more accurate the estimate of encryption efficacy [14].

### *B. Firewall*

Firewalls protect against external cyber attackers by shielding the computer or network from malicious or unnecessary network traffic. They can also prevent malicious software from accessing a computer or network via the internet. Firewalls can be configured to block data from certain locations (i.e., computer network addresses), applications, or ports while allowing relevant and necessary data through [15].

Without firewall protection, the network is not monitored for possible threats or untrustworthy communications and allows anybody to access it. Also, the sensitive data can be stolen, leaked, encrypted for ransom, or erased. Additionally, Malicious criminals might easily cause harm to businesses without proper defense [16].

To make the firewall more effective, firewall rules should be created or modified to match the needs of the user or organization, indicating which types of traffic are allowed and which are not [20].

### *C. Virtual Private Network*

A virtual private network (VPN) enables a user to connect to a private network safely via the Internet. VPN creates an encrypted connection called a VPN tunnel through which all internet traffic and conversations flow [17].

In public Wi-Fi, sensitive data may be captured by someone else on the network. A VPN encrypts the data so that others cannot read or access it [18]. Advertisers may also be watching the victims' online activity information using cookies and other tracking technologies. This information is then used to display targeted advertisements. A VPN encrypts the data, so that advertisers cannot monitor you [18].

There are many ways to improve the VPN's effectiveness, such as implementing MFA, using OpenVPN protocol, kill switch, and network lock.

VPNs provide a variety of protocols, offering different levels of protection. So, selecting the appropriate protocol is critical, and OpenVPN provides the best security and privacy. It's also rather fast, and recovering from dropped connections is quick [19].

If your VPN connection fails, you may have to use your ISP's unprotected connection. A kill switch prevents this by quickly stopping apps and restricting website access when the connection is terminated.

If your Wi-Fi network breaks, a network lock prevents your computer from connecting to the internet. This ensures that information remains confidential and secure while the VPN is adjusted.

### *D. Human Factors*

The human factor, including user and employee behavior, significantly impacts organizations' cyber security environment.

Human vulnerabilities, such as those susceptible to social engineering and phishing emails, are routinely exploited by attackers. Human factors remain the leading cause of cybersecurity breaches [20].

Inadequately trained employees may fall for phishing emails with suspicious links or attachments, leaving their systems vulnerable to malicious activities. Furthermore, employees may inadvertently disclose sensitive data, such as sending an e-mail to the wrong address [20].

Security awareness training can considerably lower the risk of this vulnerability. It is also necessary to develop a cyber security plan that considers human behavior [20].

To show the effect of human factors on phishing attacks, a survey [21] is conducted. There were twenty-six participants from the Department of Computer Engineering at Atılım University. The results are summarized below.

In the first part of the survey, some websites were chosen randomly, their URLs changed, and some of their user interface. The participants must examine them carefully and pick the left or right image as safe. In this part, the participants' accuracy is 84.61%, with 220 TRUE and 40 FALSE answers (10 image classifications per participant).

In the second part of the survey, participants are asked to choose whether the given email is safe or not, and according to their answers, two tables are extracted.

Table 1. The Accuracy, Danger and Paranoid Rate

| | **Rates** |
|---|---|
| **Accuracy** | 75.64% |
| **Danger[1]** | 13.59% |
| **Paranoid[2]** | 10.77% |

(1): This word refers to incorrect decisions, which are dangerous decisions. Those decisions may cause cybersecurity risks. (2): This word refers to wrong decisions which are not dangerous.

As shown in Table 1, 13.59% of the participants tend to make precarious decisions. Furthermore, 10.77% exhibit a propensity for erroneous decisions. The remaining portion of the participants engage in their usage practices securely.

Table 2. Safe and Dangerous Matrix

| | **Predict SAFE** | **Predict DANGER** |
|---|---|---|
| **Actual safe** | 114 | 42 |
| **Actual danger** | 53 | 181 |
| **Inaccuracy Rates** | 31.74% | 18.83% |

In the second table, when we compare the number of paranoid decisions to the total number of safe cases (156), we observe an approximate error rate of 18.83%. In cases where a safe judgment is made, there is an error margin of 31.74%.

This is a significant risk since people are prone to errors at this rate. However, it is important to note that they do not encounter as many dangerous situations as in our survey. Looking at the overall estimation rate, we have an accuracy rate of 75.6%.

## 5. GUIDELINES

This guideline aims to define ways of mitigating cyberattacks that are defined above by providing a set of safety guidelines for all employees working remotely.

### *A. User Awareness and Responsibility*

Remote workers must be vigilant about the potential loss or theft of their devices. In the event of loss or theft, employees should be aware of the proper reporting procedures. These procedures can be divided into a few steps: The employee must know where to report the incident, the reporting should be done in predetermined hours to the responsible unit, and the reported device must be fully wiped out remotely. When using work devices, employees should refrain from altering settings, installing unauthorized software, or removing storage space on their work devices. Employees should not grant family members or other individuals access to their work devices. If work devices contain critical company information, they should be stored on the company's servers and not their computers. Remote workers must use company-authorized antivirus software. Employees should be aware of using their personal devices for work purposes. Additionally, they should be cautious of phishing attempts sent to their email and should carefully check links and not click on links or attachments they do not trust. To become a conscientious user, staying informed about current cyber threats is imperative. This increases user awareness and preparedness to navigate the evolving landscape of cybersecurity challenges.

### *B. Remote Working Area Arrangements*

The employees should be aware of the threats to their physical security and risks while working from a mobile working location. The portable computing device, which contains the data of the work, should be located in a place that will not increase the interest of an opportunity seeker thief or a casual visitor to the work area. In addition to the device itself, the login credentials to that device or any app in that device and any kind of identification information should be located in a separate place by the employee. Apart from portable computing devices, any printed document should be stored in a case that does not allow casual reading. Also, the paper contains restricted or protected information, but now, waste must be shredded.

### *C. Access Control and Management*

During remote working, employees generally have access to the sensitive data labeled as to be protected or restricted and the employees have responsibilities towards this kind of information such as the security of the file. In order to satisfy this responsibility, there are control mechanisms such as physical and technical. Appropriate approaches to the physical control mechanism are mentioned in section B. As to the technical control mechanism, there are several steps to provide this mechanism, such as user login controls, data encryption, secure connection, MFA, etc. To provide user login controls, the employee must use password controls to the whole device, and if not possible, the sensitive data must be protected by the password. The password provided by the employee must be strong. To ensure this, the employee should avoid using passwords that are reused, shared, or passwords that do not contain special characters, lower/upper case letters, and numeric. As to data encryption, if possible, whole documents in the portable device must be encrypted repeatedly, but if it's not possible, the files that contain sensitive data must be encrypted. MFA, in this case DFA (double factor authentication), is critical to mitigate malicious cyber-attacks [22]. As to the last technical mechanism, secure connection, there are two steps to achieve this: using VPN/SSL and proxy servers. An SSL or IPSec VPN must be configured to provide protection whenever an employee tries to access sensitive information via a public network. In the second step, if an employee is working in an organization, the connection must be done by a proxy server provided by an organization instead of a public network.

### *D. Security Tools*

Utilizing updated antivirus software -with an updated operating system and firewall can effectively shield remote workers' computers from a range of threats, including malware, keyloggers, and phishing software or websites. Furthermore, employing artificial intelligence-based protection mechanisms can provide a robust defense against evolving phishing techniques and scam emails. Additionally, integrating password manager and generator tools into security protocols offers an extra layer of protection by securely storing and creating strong, unique passwords for various accounts, thereby mitigating the risk of credential-based attacks.

## 6. CONCLUSION

In conclusion, this article aimed to raise the awareness of cybersecurity threats by explaining them individually. Additionally, the questionnaire shows current awareness of phishing attacks. In the related sections, the ways and tools to mitigate the cybersecurity threats are explained with ways to make them more effective and showing what might happen in case of their absence. As a last section, a complete guide is suggested for remote workers to explain ways to mitigate cyber threats in different areas.

## REFERENCES

[1] N.A. Rakha, Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices, vol. 1, issue. 3, International Journal of Law and Policy, 2023.https://doi.org/10.59022/ijlp.43

[2] Z. Khan and P. Charan, Work-from-home Security Issues and Risk over Internet, pp. 468–472, 2023 DOI:10.47715/JPC.B.978-93-91303-45-7_81

[3] S. Senapati and S.V. Baharatti, An Empirical Study on the Information Security Threats Due to Remote Working Environments. In: Kulkarni, A.J., Cheikhrouhou, N. (eds) Intelligent Systems for Smart Cities. ICISA 2023. Springer, Singapore, 2024. https://doi.org/10.1007/978-981-99-6984-5_2

[4] S. Milson and B. Altan, Cybersecurity in Remote Work Environments: Challenges And Best Practices. [Online]. Available: http://www.ctan.org/tex-https://easychair.org/publications/preprint_download/9lj5

[5] B. Buckley, Securing a Remote Workforce, University of New Hampshire, Manchester, June 15, 2021. Available: https://static1.squarespace.com/static/60d4f2e1ecf6cb1c708d572b/t/60f16cabe7c78223958b9089/1626434731404/Buckley+898.M1_+Capstone+Final+Draft.pdf

[6] S. A.A.D. Effective information security policies for efficient remote working : Software professionals' perspective, [Master's theses, University of Moratuwa]. Institutional Repository University of Moratuwa, 2019. Available: http://dl.lib.uom.lk/handle/123/16362

[7] C. Vásquez and J. González Cybersecurity engagement in a remote work environment [Online]. Available: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9090426&fileOId=9090427
[8] J. Hong, The state of phishing attacks, Commun. ACM, vol. 55, no. 1, pp. 74–81, Jan. 2012. Available: doi: 10.1145/2063176.2063197
[9] R. Richardson and Max M. North. Ransomware: Evolution, Mitigation and Prevention'. [Online]. Available: https://digitalcommons.kennesaw.edu/facpubs/4276/
[10] F. Aliyu, T. Sheltami and E.M. Shakshuki, A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing, vol 141, pages 24-31, 2018. Available: https://doi.org/10.1016/j.procs.2018.10.125
[11] R. Muppavarapu, *Open Wi-Fi hotspots- Threats and Mitigations*. [Online]. Available: https://dl.packetstormsecurity.net/papers/wireless/openwifimitigations.pdf
[12] S. Weamie, *Cross-Site Scripting Attacks and Defensive Techniques: A Comprehensive Survey*, International Journal of Communications, Network and System Sciences, vol. 15, pp. 126–148, Aug. 2022. Available: DOI: 10.4236/ijcns.2022.158010.
[13] World Economic Forum (2022) The Global Risks Report 2022 17th Edition. Insight Report.[Online]. Available: https://www.weforum.org/publications/global-risks-report-2022/
[14] Linkedin *How do you measure the effectiveness of your encryption?*. [Online]. Available: https://www.linkedin.com/advice/3/how-do-you-measure-effectiveness-your-encryption
[15] CISA. Cybersecurity and Infrastructure Security Agency. *Understanding firewalls for home and small office use*. [Online]. Available: https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use
[16] M. S. Villanueva. *3 Top Risks of Not Having a Firewall*. [Online]. Available: https://www.itsasap.com/blog/3-top-risks-of-not-having-a-firewall
[20]J. Pioth, *How to Make a Firewall Effective*. [Online]. Available: https://www.coeosolutions.com/news/make-firewall-effective
[17] GeekForGeeks(2023), Types of Virtual Private Network (VPN) and its Protocols. [Online]. Available: https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/
[18] A. Brown (2022), These 4 Things Could Happen If You Don't Use A VPN. [Online]. Available: https://southernmarylandchronicle.com/2022/04/27/these-4-things-could-happen-if-you-dont-use-a-vpn/
[19] Linkedin(2024), What VPN performance strategies can remote workers use to improve productivity?. [Online]. Available: https://www.linkedin.com/advice/0/what-vpn-performance-strategies-can-remote-gtmpe
[20] D. Bell(2023), The Human Element in Cybersecurity: Understanding Human Factor in Cyber Threats. [Online]. Available: https://www.linkedin.com/pulse/human-element-cybersecurity-understanding-factor-cyber-david-bell-jezuf?trk=article-ssr-frontend-pulse_more-articles_related-content-card#:~:text=The%20human%20factor%2C%20including%20both,are%20often%20exploited%20by%20attackers
[21] Phishing Attack Survey. [Online]. Available: https://forms.gle/Pw2G1vCiBJQ4t1hQ7

[22] CSA (2022), Weak Security Controls and Practices Routinely Exploited for Initial Access. [Online] Available: https://media.defense.gov/2022/May/17/2002998718/-1/-1/0/CSA_WEAK_SECURITY_CONTROLS_PRACTICES_EXPLOITED_FOR_INITIAL_ACCESS.PDF