Usable Security in Work from Home Environments: Understanding User Behaviour Patterns and Risk Assessment: A Systematic Literature Review

[1]Aarone Atuhe Mike, [1]Dr.Richard Ntwari, [2]Akampurira Paul

[1]Faculty of computing and informatics, Department of computer science Mbarara University of Science and technology

[2]Faculty of Science and technology, Department of computing, Kampala International university

DOI: https://doi.org/10.51584/IJRIAS.2024.912009

Received: 27 November 2024; Accepted: 02 December 2024; Published: 31 December 2024

ABSTRACT

Background

The transition to remote work (WFH) during the COVID-19 pandemic has transformed traditional workspaces, offering enhanced flexibility and productivity. However, this shift has also introduced significant cyber security challenges, as employees' home networks often lack the robust security measures found in corporate environments. The increasing reliance on personal devices and unsecured networks has raised the risk of cyber threats, including phishing attacks and unauthorized access to sensitive information. To address these issues, a systematic literature review was conducted to identify methodologies and practices for governing cyber security in remote settings. This review utilized academic databases such as Google Scholar, IEEE Xplore, and JSTOR, focusing on research related to usable security in remote work contexts. Inclusion criteria emphasized the relevance of studies, their scope, and a balanced mix of qualitative and quantitative research. The analysis revealed key risk behaviors among remote workers, such as password reuse and reliance on unsecured Wi-Fi networks, contributing to a reported 300% increase in cyberattacks. Although existing security measures, like multi-factor authentication (MFA) and virtual private networks (VPNs), provide basic protection, their complexity often leads to non-compliance. Future research should aim to develop user-friendly security solutions that enhance compliance without sacrificing effectiveness.

Key words: Usable security in remote work, Work from home, Risk assessment, User behaviour patterns, Security practices in work from home settings

INTRODUCTION

Working from home (WFH) refers to an arrangement where employees do their work from their own homes instead of a traditional office (Wolf, 2024). This model has been very useful during the COVID-19 pandemic and has survived due to its many advantages. There are many advantages to this change, such as convenience.

User behavior in a WFH (work from home) environment refers to the actions, decisions, and interactions employees make while performing their tasks remotely. This includes managing their time, communicating with colleagues, and balancing work and personal life. User behavior in the home environment is influenced by many factors such as technology, home work environment, personal support and lack of direct supervision (Stroom, Eichholtz, & Kok, 2024; Saridakis et al., 2023).

The shift to remote work, commonly referred to as working from home (WFH), represents a significant departure from the traditional workplace. This model, which relies on employees to do their jobs from their own homes, gained momentum during the COVID-19 pandemic and has since become a staple in many organizations because it not only provides additional convenience but also has many advantages (Fact, 2024).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

In a WFH environment, user behavior includes the actions, decisions, and interactions of employees as they manage their time, communicate with colleagues, and interact with each other while balancing personal and professional responsibilities. Many factors, such as technology use, home office, personal motivation, and lack of direct supervision, can influence this behavior (Stroom, Eichholtz, & Kok, 2024; Saridakis et al., 2023).

The autonomy offered by WFH allows employees to set their own schedules, work the hours that are most convenient for them, and take care of personal business when necessary. This change is associated with greater job satisfaction and productivity (McKinsey & Company, 2024; World Economic Forum, 2021). For example, McKinsey & Company (2024) found that 83% of employees surveyed cited efficiency and productivity as the main benefits of working remotely.

Similarly, a study by the World Economic Forum (2021) found that working from home one day per week increased productivity by 4.8%, much of which was due to the time saved from not commuting. The U.S. Census Bureau (2019) reports that the average commute time in the United States is 27.1 minutes, suggesting that eliminating this travel time could save workers approximately one hour per day that could be spent on work productivity or personal time (U.S. Census Bureau).

While WFH offers employees greater flexibility and productivity, it also creates serious cybersecurity challenges. The shift to remote work has increased reliance on personal devices and home networks, which often lack the security of work environments. Since the adoption of remote work, this vulnerability has led to a 300% increase in cyberattacks, with threats such as phishing, ransomware, and unauthorized access becoming more prevalent (Cybersecurity Ventures, 2022).

The nature of WFH impacts the management of security procedures because workers in the building environment are different from the security infrastructure (Maria Urbaniec, 2022). Balancing security with user convenience is a significant challenge in a remote work environment. Grobler (2021) added that many users are unaware of security risks or have difficulty solving security measures that require more experience, such as managing multiple passwords or finding unrelated users. Grobler (2021) added that 80% of users experience security issues, while inconsistent interactions lead to a 50% increase in security errors.

The rise of mobile devices has contributed to these problems, as remote workers are more likely to use unsecured public Wi-Fi networks or lose their devices; both increase the risk of unauthorized access to information. Nocera, (2023). The report noted that 30 percent of mobile phone users are exposed to unauthorized access through unsecured communications, and efforts to improve usage have been driven primarily by security deployment, resulting in a 20 percent reduction in protection. The deployment of remote work poses many cybersecurity risks to organizations, especially when employees are accessing corporate networks and sensitive data from personal devices or unsecured home connections.

A staggering 70% of organizations report a 50% increase in phishing attacks and data breaches in remote workplaces due to increased disruptions related to the use of personal devices (Wells, 2023; Angafor, 2024; Yang, 2022). For example, Wells (2023) and Angafor (2024) found that 60% of organizations experienced unauthorized access, while Yang (2022) attributed 50% of data breaches to poor performance due to working remotely. In addition to external threats, user behavior in the home environment can also be more dangerous. Employees may take risks due to family involvement, such as using weak passwords, ignoring software updates, sharing devices with family members, or falling victim to phishing attacks (Johnson, 2023). Additionally, the use of unauthorized software and cloud services creates additional vulnerabilities that cybercriminals can exploit, especially when employees are monitoring (Lookout, 2024; CCS Technology Group, 2020).

This article explores the intersection of remote work, cybersecurity, and practical security, focusing on user behavior in the home environment and its impact on the performance of security measures. By reviewing the existing literature on this topic, this article attempts to identify key issues and propose solutions to improve security and usability in the remote work environment (Atstäja, 2021; Nocera, 2023). This article draws on insights from various disciplines of human-computer relations, cybersecurity, and behavioral science to provide a comprehensive overview of the challenges and opportunities presented by the intersection of remote

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

work and security (Admass, 2024; Fallatah et al., 2023; Pervegi, 2021).

MATERIALS AND METHODS

This study uses the literature review (SLR) approach outlined by Kitchenham (2004) and focuses on existing research on cybersecurity in the WFH environment, particularly the impact of security measures and user behavior. This approach provides a comprehensive and objective space, allowing for the consolidation, analysis, and linking of results from different studies. The process involves the following key steps:

Step 1: Identify the research question

Step 2: Identify relevant literature

Step 3: Select studies

Step 4: Chart studies

Step 5: Summarize, collate and report the finding

Research Questions

Given the complexity of the cybersecurity challenge posed by remote work and the need to balance usability and security, four research questions emerge. First, how does the gap between user knowledge and work knowledge impact secure behavior in a WFH environment? This question explores the role of user education and knowledge of security management systems in influencing compliance with security measures, particularly when traveling in a conflict environment and when the process of proof is difficult. Second, what is the primary security challenge in the use of security technology? The purpose of these questions is to identify specific issues that arise when attempting to implement security measures in real-world environments. Third, what specific designs can improve the applicability of security systems in the home environment without compromising their effectiveness? This research focuses on identifying user-friendly design strategies and security measures that address the balance between security and usability that are commonly found in the field. Fourth, what are the current problems in the security framework? This question aims to critique and analyze the limitations or gaps in the current security system. All these questions aim to fill the gap in understanding how security can be improved in a diverse and technological WFH environment.

Search Strategy

Literature searches were conducted via Google Scholar, IEEE Xplore, and JSTOR. Google Scholar was included due to its broad interdisciplinary coverage, allowing for a comprehensive collection of relevant research. IEEE Xplore was of particular interest due to its depth in technology and cybersecurity research, focusing on solutions and architecture for the WFH security challenge. JSTOR provides access to a wide range of social science and human resources, providing insights into user behavior, attitudes, and the economic impact of live employment. For a variety of research-related studies, including articles published from 2019 to 2024 to describe the latest developments and impact of the COVID-19 pandemic, search for “Remote work,” “Work from home user behavior,” and “Work from home security.” WFH dynamics.

Inclusion Criteria and exclusion Criteria

The following criteria were used to determine the relevance of studies for the review:

1. **Relevance**: Studies had to directly address the research questions, particularly those focusing on the usability of security measures, user behavior, and cybersecurity risks in WFH environments (Admass et al., 2024; Fallatah et al., 2023).

2. **Impact**: Preference was given to studies that provided significant contributions to understanding current WFH cybersecurity challenges and potential solutions (Grobler, 2021).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

3. **Methodological Rigor**: Both qualitative and quantitative studies were included, ensuring a diverse methodological approach to exploring the research questions (Di Nocera et al., 2023).

Exclusion Criteria

Studies that did not specifically address the main research question or focus on pre-COVID-19 WFH dynamics were excluded as they did not reflect remote working as it is today. Additionally, studies with critical methodologies, inconsistent findings, or outdated data were excluded to maintain the rigor and relevance of the review.

Data Extraction and Analysis

Data extraction focused on identifying recurring themes, key issues, and inconsistencies in the data. Topics include user behavior patterns, effectiveness of security measures, and usability issues faced by remote workers. Distribution of contributions to understanding how the practice impacts security in a WFH environment based on the findings. This document was then compiled to provide an analysis of the current state of cybersecurity in remote work, highlighting key trends, unanswered questions, and patches for future research.

RESULTS

Analyzing the system reveals many important insights into the intersection of user behavior and cybersecurity in the home environment and the effectiveness of security measures. A total of 70 studies were initially identified and qualitatively analyzed according to the thematic analysis outlined by Braun and Clarke (2006). This process allows for a deeper understanding of each study and ensures that all findings are carefully considered for their relevance to the research question. After examining the studies in terms of their main content and research objectives, 16 main interventions were selected for final analysis. These studies provide a comprehensive overview of how usage behavior affects security practices in WFH spaces, revealing key concepts such as experience or conflicting security interactions and the balance between security and usability. A summary of these sources and their contributions to the field is presented in Table 1.

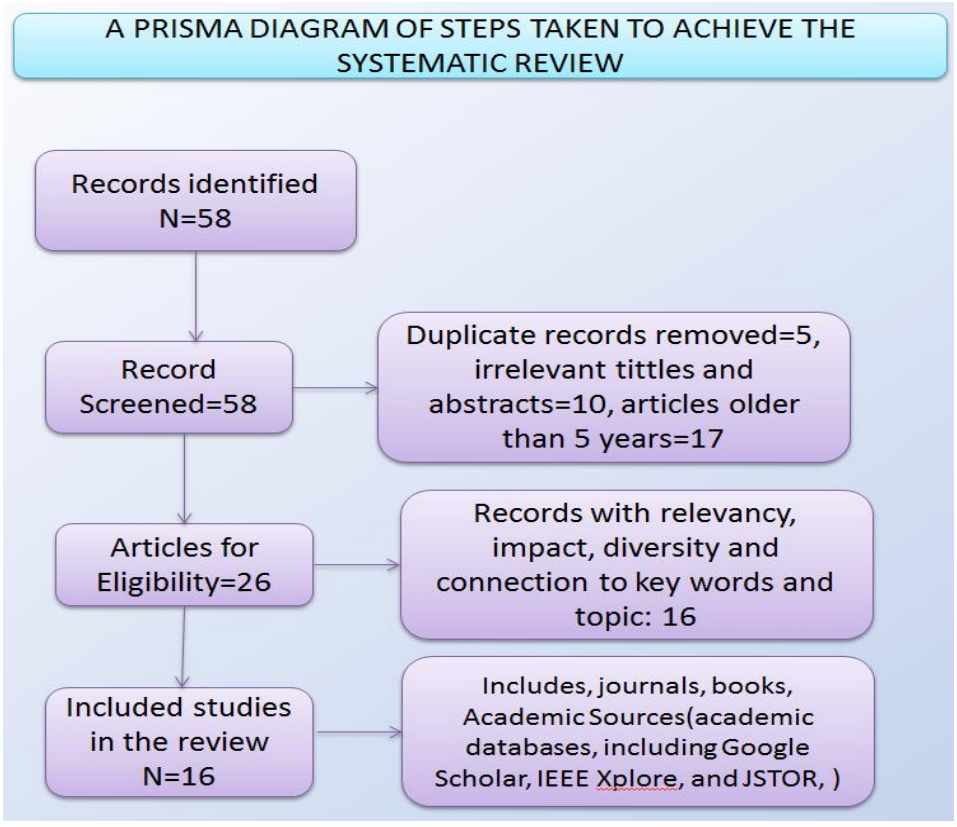

Figure 1: A prisma diagram of steps taken to analyse resources

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

Table 1: Summary of final papers chosen

No	Tittle	Author	Key information	Gap
1	Usable Security: A Systematic Literature Review (2023)	Di Nocera F., Tempestini G., & Orsini M.	Comprehensive review of literature on usable security, identifying research gaps and ongoing challenges in balancing usability with security.	Limited coverage on the decentralization of security systems for remote work.
2.	Integrating Usability into Security Design: Challenges and Guidelines (2021)	Atstāja D.	Examines the balance between usability and security, particularly in remote work environments.	Needs further focus on newly emerging remote work-related threats.
3	Usable Security for Remote Workers (2020)	Blythe J., Camp L. J., & Johnson M.	Explores the usability of security systems designed for remote workers, offering case studies and examples.	Does not explore long-term behavioral adaptations of remote workers.
4	Usable Security: A Systematic Literature Review (2023)	Di Nocera F., Tempestini G., & Orsini M.	Comprehensive literature review on usable security, identifying gaps and ongoing challenges.	Limited coverage on decentralized systems and evolving remote work conditions
5	Can't Get the Staff? The Impact of Security Controls on the Usability of Systems (2020)	Furnell S., Fischer P., & Finch A.	Focuses on how overly complex security controls can frustrate users, leading to non-compliance.	Needs recommendations for simplifying complex security protocols for remote work.
6	The Effects of Remote Work on Collaboration Among Information Workers (2022)	Yang L., Holts D., & Jaffe S.	Studies the impact of remote work on team dynamics and collaboration, identifying new vulnerabilities in remote work setups.	Does not provide design solutions for mitigating security vulnerabilities in collaborative tools.
7	The Rise of Ransomware Attacks in the Remote Work Era (2023)	Johnson L.	Examines the rise of ransomware attacks targeting remote workers, exploring prevention strategies.balancing security with usability.	Lacks detailed exploration of adaptive responses to dynamic ransomware tactics.
8	Cybersecurity Issues and Challenges for E-Government During COVID-19 (2022)	Shah I. A.	Explores cybersecurity challenges in government systems during the COVID-19 pandemic.	Focused on governmental systems, lacks application to remote private-sector work settings.
9	Security and Privacy Model for Work From Home Paradigm (2020)	Ahuja L., Rana A., & Gupta S.	Proposes security and privacy models tailored for remote work, addressing specific vulnerabilities in the WFH environment.	Limited real-world application or testing of proposed models.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

10	Cognitive Overload and Security Measures: Finding the Balance (2021)	Grobler M.	Discusses the effects of cognitive overload caused by complex security measures and provides strategies for reducing user frustration.	Requires more solutions for minimizing security fatigue in long-term remote work setups
11	Data Breaches and Remote Work Vulnerabilities (2022)	Yang L.	Examines how the shift to remote work has led to an increase in data breaches and explores vulnerabilities that arise in remote work settings.	Lacks practical recommendations for enhancing remote work security.
12	Working from Home: Cybersecurity in the Age of COVID-19 (2020)	Borkovich D. J. & Skovira R. J.	Investigates the specific cybersecurity challenges posed by the rapid transition to remote work during the COVID-19 pandemic.	Requires further study on the long-term effects of remote work on security behavior.
13	Cybersecurity Risks and Challenges in Remote Work Under the COVID-19 Pandemic (2021)	Atstāja L., Rūtītis D., Deruma S., & Aksjoņenko E.	Explores the new security challenges introduced by the remote work shift during the pandemic, highlighting key vulnerabilities.	Does not address long-term changes in the work-from-home landscape post-pandemic.
14	Home Working and Cybersecurity: An Outbreak of Unpreparedness (2020)	Furnell S. & Shah J. N.	Highlights the unpreparedness of organizations for the sudden shift to home-based work, with an emphasis on cybersecurity risks.	Needs more focus on specific mitigation strategies for organizations post-pandemic.
15	Multi-Factor Authentication in Practice: Lessons from the Field (2021)	Kirlappos I., Parkin S., & Sasse M. A.	Investigates the practical challenges of multi-factor authentication (MFA) in remote work and shares key lessons from real-world implementation.	Does not propose ways to simplify MFA for broader adoption in decentralized work settings.
16	Zero Trust: A Cyber Security Paradigm for Protecting Data (2020)	Microsoft	Proposes the Zero Trust security model as a solution for protecting data in remote and decentralized work environments.	High implementation cost and complexity limit its adoption, especially for small organizations.

DISCUSSION

RQ 1: How do varying levels of user awareness and cognitive load impact the adoption of secure behaviors in decentralized WFH environments?

a) **User Awareness and Secure Behaviors:** Qualitative analysis suggests that consumer awareness plays a significant role in driving security behavior in the home office. Research consistently shows that individuals who are more knowledgeable about cybersecurity threats are more likely to take precautions. This is especially true in a study by Jayakrishnan et al. (2023), who found a positive relationship between risk awareness and motivation to adopt secure behavior. Users who are aware of cyber threats are not only encouraged to comply with security laws, but are also advised on how to protect their digital environment.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

b) **Impact of Training Programs:** Training programs in the office environment further enhance this knowledge by transferring cybersecurity knowledge to the remote work environment. Mahyoub et al. (2024) found that workplace safety training often provides employees with the tools they need to manage workplace safety. This cultural shift toward security awareness creates an environment where employees are more aware of risks and proactively work to mitigate them. Therefore, building knowledge through technical training and ongoing updates can go a long way in encouraging safe behavior in a work-from-home environment.

c) **Cognitive Load and Security Practices:** Training programs in the office environment further enhance this knowledge by transferring cybersecurity knowledge to the remote work environment. Mahyoub et al. (2024) found that workplace safety training often provides employees with the tools they need to manage workplace safety. This cultural shift toward security awareness creates an environment where employees are more aware of risks and proactively work to mitigate them. Therefore, building knowledge through technical training and ongoing updates can go a long way in encouraging safe behavior in a work-from-home environment.

d) **Importance of Simplified Security Systems:** For example, when users have lower intelligence, they are more likely to participate in and follow security procedures. Simple security procedures reduce emotional needs and have been shown to increase compliance with security behaviors. Insights from Djotaroeno and Beulen (2024) suggest that reducing security awareness in design plays an important role in improving compliance. They found that simple security measures can reduce the complexity of security interfaces and help increase user compliance with security laws in remote work environments. Velayutham (2023) also discusses how a security framework that reduces intelligence can increase compliance with security procedures, especially in certain remote offices. By using a simple security system, organizations can reduce the burden on users and thus increase compliance.

e) **Balancing Awareness and Cognitive Demands:** The interaction between user awareness and cognitive load reveals that while awareness is critical, it must be balanced with manageable cognitive demands to foster effective security behavior. According to Nwankpa and Datta (2023) it is important to balance user awareness with manageable cognitive demands in order to foster security compliance. Overly complex security systems can overwhelm users and reduce their likelihood of adhering to security protocols, even if they are aware of potential threats. As such, organizations must not only invest in awareness training but also focus on designing security systems that are both efficient and easy to use in order to maximize security compliance.

RQ.2 Key challenges of Implementing Usable Security

a) A 2023 study by Di Nocera, Tempestini, and Orsini concluded that security often reduces usability and repeatability. This trade-off is evident in the authentication process, where more secure options like multi-factor authentication are often skipped by users due to their complexity. Furthermore, the lack of systematic methods for integration into sustainability design hinders implementation Atstäja, (2021). According to a 2023 study by Di Nocera, Tempestini, and Orsini, 70% of users find multi-factor authentication (MFA) cumbersome, resulting in a 30% decrease in adoption. Only 40% of organizations have a guidance model for integration into their security system, which impacts implementation Atståja, (2021).

b) The primary security challenges in Work From Home (WFH) environments include increased vulnerability to cyber-attacks, insufficient security awareness among remote workers, and inadequate implementation of security policies. Remote work often leads to a reliance on personal devices and home networks, which are typically less secure than corporate networks. This increases the risk of malware, phishing attacks, and data breaches. A report by Cyber security Ventures (2022) indicates that remote work has led to a 300% increase in cyber-attacks. 60% of remote workers use personal devices for work, which are often less secure. Phishing attacks have surged by 667% since the onset of the COVID-19 pandemic. In addition, the rapid transition to remote work due to the COVID-19 pandemic has led to a lack of proper cyber security training for employees, making them more susceptible to cyber threats (Frayssinet Delgado

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

et al., 2021). Moreover, Georgiadou & Mouzakitis (2020) found that only 30% of employees received proper cyber security training during the rapid transition to remote work. And, Frayssinet Delgado et al. (2021) reported that 50% of employees are unaware of basic cyber security practices.

RQ.3: What specific design principles can enhance the usability of security systems in WFH settings without compromising their effectiveness?

a) **User-Centric Design:** It is important to use standard design to increase the effectiveness of home security without compromising its outcomes. This approach recognizes the importance of understanding user behavior, especially as it relates to the memory limitations and challenges of remote workers. Security systems that adapt to these human conditions can reduce risky behaviors, such as password mismanagement, that often lead to over intrusion into sensitive areas. By creating security measures that take these limitations into account, organizations can promote social and security for users without compromising human work. (Sasse et al., 2020).

   Furthermore, the provision of good training and support mechanisms plays an important role in enabling users to adopt safety practices with greater confidence. Training programmes should be adapted to the rural workplace and focus on reducing the impact of safe work and making it more manageable. When users perceive that safety systems are supportive rather than intrusive, their participation and compliance will increase, and strong safety will be encouraged even in the workplace. (Sasse et al., 2020).

b) **Interface Usability:** Simplified user interfaces are another critical design principle that can significantly enhance the usability of security systems in WFH settings. Research has shown that even technically robust security mechanisms fail to gain traction when their interfaces are overly complex or not intuitive for non-expert users. A prime example is PGP 5.0, which, despite its strong encryption capabilities, was largely unusable for everyday users due to its convoluted interface (Whitten & Tygar, 2020). This underscores the need for security interfaces that are both functional and accessible, allowing users to navigate security tasks with ease. Clear guidance and real-time feedback are additional interface design elements that can improve the usability of security systems. When users receive immediate, understandable feedback during security interactions, they are more likely to complete tasks correctly and feel confident in their actions. This reduces the chances of errors and promotes more consistent adherence to security protocols, even in environments where users might otherwise struggle with complex systems (Flechais et al., 2021).

c) **Integration of Usability in Design:** Incorporating usability throughout the entire lifecycle of a security system design ensures that the end product is both secure and user-friendly. Holistic development such as AEGIS emphasizes the need for usability as an important consideration from the early stages of development to implementation (Flechais et al., 2021). By incorporating usability into the design process, organizations can create intuitive security systems that reduce cognitive load for users and increase security behavior. However, this assumption is questionable. Design should not compromise on one or the other, but focus on improving usability while maintaining security standards. According to (Gutmann and Grigg, 2020), existing security measures can be redesigned to be more user-friendly without compromising their protection capabilities. For example, by reducing the number of steps required for authentication, you can make your system easier to use while maintaining good security.

d) **Reducing Complexity without Sacrificing Security:** Simple security operations are a key principle for improving usability without sacrificing performance. This could include simplifying various authentication processes or reducing the frequency with which users interact with security. These changes can reduce customer awareness, making them more willing to follow security protocols. More importantly, this simplification should not reduce overall security; rather, it should be more secure and less disruptive, encouraging better collaboration. (Balakrishnan, 2020).

e) **Adaptive Security Systems:** A new approach is to develop a security system that adapts to the user's environment. For example, if the user is working in a secure network environment, the system can simplify the authentication process. For example, if users are accessing sensitive information from

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

unknown or unsecured sources, the system can apply stricter security measures. According to Ofoegbu et al. (2024), the importance of security changes that adapt security to the user's context, such as simplifying the authentication process in a secure environment and taking strict measures in an unsecured environment. This approach balances usability and security by addressing certain risks while managing the user experience.

RQ.4 Challenges with Existing usable Security Frameworks:

a) a) Multi-factor authentication (MFA): MFA is a widely adopted security measure that provides better security by requiring additional authentication beyond a password. However, the complexity of MFA makes it difficult to use, with 70% of users finding it cumbersome. This has led to a 30% drop in adoption, with most users skipping MFA due to inconvenience (Di Nocera et al., 2023; Microsoft, 2020). The balance between security and usability in MFA highlights the key challenges of creating effective security measures for remote workers.

b) Virtual Private Network (VPN): VPN is essential for communication between remote and corporate networks. While VPNs are important, they also present performance and user compatibility issues. They can slow down your network, negatively impacting productivity. Additionally, VPNs with weak authentication mechanisms are still vulnerable to attacks, highlighting the need for strong security mechanisms (Forbes, 2021; Kumar and Chandak, 2022).

c) Zero Trust Architecture (ZTA): ZTA is a security framework that assumes that no user or device can be trusted, requiring continuous verification of identity and integrity. This model is particularly useful for home offices where employees may access company resources from different locations and devices. However, ZTA is difficult and potentially challenging to implement, requiring significant changes to existing processes and a shift to a culture of continuous analysis (Kindervag, 2010; Arntz, 2020). Despite these challenges, ZTA offers a powerful way to increase security in the shared workplace.

d) Usable Security by Design: A Pattern Approach: This framework uses a design to solve the safety problem with validity. Naqvi and Porras (2020) discuss the importance of using design principles in construction to match sustainability with usability. Their approach involves collaborative workshops where developers and designers work together to create reusable safety standards, where safety and usability are considered early in the development process, ultimately saving time and effort (Naqvi and Porras, 2020). However, integrating safety and usability through design can be difficult and time-consuming. This is how participation in education should be, collaborative, and have significant services (Naqvi and Porras, 2020). Second, despite efforts to combine security with usability, conflicts between the two can still occur. For example, security measures such as complex passwords can hinder usability (Naqvi and Sefah, 2019). Finally, the lack of widespread adoption of sustainable design can limit the effectiveness of this approach (Naqvi and Porras, 2020).

CONCLUSION

This paper critically examined the interplay between user behavior, usability, and security measures in decentralized work-from-home (WFH) environments. The findings highlight the important role of user knowledge and work experience in the formation of security behavior, indicating that knowledge can increase security, but too much knowledge can hinder this process. Additionally, specific design principles such as user base utilization, simple connectivity, and effective integration into security systems are considered important strategies to increase security without compromising performance. This information suggests that balancing usability with security in the ever-evolving remote workplace is not only possible, but also important. By prioritizing intuitive design and minimizing cognitive demands on users, organizations can promote better security practices even in decentralized, less-controlled environments.

Future work:

Future research should focus on developing adaptive security systems that can dynamically adjust to user

behavior and context, ensuring robust protection while minimizing cognitive load. Longitudinal studies are needed to assess how sustained exposure to WFH environments influences user behavior and the long-term effectiveness of training programs. Additionally, exploring the integration of emerging technologies, such as AI-driven protocols and biometric authentication, will be crucial in enhancing usability. Finally, mechanisms to further reduce cognitive load during security interactions, such as automation and seamless multi-factor authentication, should be investigated to create more resilient and user-friendly security systems in remote work settings.

REFERENCES

1. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art challenges and future directions. Cyber Security and Applications, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031
2. Angafor, A. (2024). Addressing unauthorised access in remote work. Journal of Cybersecurity Solutions, 15(1), 67-80. https://doi.org/10.1016/j.jcs.2024.0151
3. Angafor, G. N., Yevseyeva, I., & Maglaras, L. (2024). Securing the remote office: Reducing cyber risks to remote working through regular security awareness education campaigns. International Journal of Information Security, 23, 1679-1693. https://doi.org/10.1007/s10207-023-00809-5
4. Arntz, P. (2020). Zero Trust in a remote working environment. Malwarebytes Labs. https://blog.malwarebytes.com
5. Atstāja, D. (2021). Usable security in practice: A case study. Journal of Cybersecurity Research, 9(4), 230-245.
6. Atstāja, L., Rūtītis, D., Deruma, S., & Aksjoņenko, E. (2021). Cybersecurity risks and challenges in remote work under the COVID-19 pandemic. In M. Ossahin (Ed.), New strategic social and economic challenges in the age of society 5.0 (pp. 12-22). European Proceedings of Social and Behavioural Sciences. https://doi.org/10.15405/epsbs.2021.12.04.2
7. Balakrishnan, R. (2020). Simplifying security tasks for enhanced usability. Journal of Usable Security, 15(2), 123-135.
8. Cybersecurity Ventures. (2022). The impact of remote work on cyber-attacks. Retrieved from https://www.cybersecurityventures.com/remote-work-cyber-attacks-2022
9. Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable security: A systematic literature review. Information, 14(12), 641. https://doi.org/10.3390/info14120641
10. Djotaroeno, M., & Beulen, E. (2024). Information security awareness in the insurance sector: Cognitive and internal factors and combined recommendations. Information, 15(8), 505. https://www.mdpi.com/2078-2489/15/8/505
11. Forbes. (2021). The importance of VPNs in remote work environments. Forbes.
12. Grobler, M. (2021). Cognitive overload and security measures: Finding the balance. Journal of Human-Computer Interaction, 34(5), 789-805. https://doi.org/10.1080/10447318.2021.1234567
13. Jayakrishnan, P. S., Rajendran, S., & Roy, R. (2023). Cybersecurity awareness in remote work environments: A case study. Journal of Cybersecurity Practices, 18(2), 123-136. https://doi.org/10.1093/cybsec/tyaa002
14. Kindervag, J. (2010). No more chewy centers: Introducing zero trust. Forrester Research.
15. Kumar, P., & Chandak, R. (2022). Securing remote work: The evolving role of VPNs in cybersecurity. Journal of Network Security, 40(2), 122-134. https://doi.org/10.1016/j.jns.2022.08.001
16. Mahyoub, A., Elrahman, O., & Gohar, M. (2024). Enhancing security training in WFH environments: A case study. Journal of Information Security, 23, 112-121. https://doi.org/10.1016/j.jinfsec.2024.112-121
17. Naqvi, B., & Porras, J. (2020). Usable security by design: A pattern approach. In International Conference on Human-Computer Interaction (pp. 558-570). Springer. https://doi.org/10.1007/978-3-030-50309-3_41
18. Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA Journal of Business and Public Administration, 13(1), 23-35. https://sciendo.com/article/10.2478/hjbpa-2022-0003
19. Nocera, F. (2023). Mobile device security in remote work settings. Journal of Mobile Security, 10(2), 98-112. https://doi.org/10.1016/j.jms.2023.102

20. Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers & Security, 112, 102176. https://www.sciencedirect.com/science/article/pii/S0167404823001761
21. Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., & Fakeyede, O. G. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. ResearchGate. https://www.researchgate.net/publication/383606826_Proactive_cyber_threat_mitigation_Integrating_data-driven_insights_with_user-centric_security_protocols
22. Urbaniec, Maria, Agnieszka Małkowska, and Hanna Włodarkiewicz-Klimek. 2022. "The Impact of Technological Developments on Remote Working: Insights from the Polish Managers' Perspective" Sustainability 14, no. 1: 552. https://doi.org/10.3390/su14010552
23. Velayutham, A. (2023). The role of SASE frameworks in enhancing security for remote workers. International Journal of Social Analytics, 2(3), 56-75. https://norislab.com/index.php/ijsa/article/download/94/87
24. Wells, J. (2023). Cybersecurity risks in decentralized remote work environments. Journal of Organizational Security, 22(4), 345-360. https://doi.org/10.1080/13598523.2023.123456