Combined Proceedings of the 39th iSTEAMS Bespoke Conference – July, 2025
& iSTEAMS Emerging Technologies onference October, 2025

Society for Multidisciplinary & Advanced Research Techniques (SMART - Scientific Projects & Research Consortium (SPaRC)
West Midlands Open University – Projects, Research, Innovations, Strategies & Multimedia (PRISM) Centre
PearlRichards Foundations- Accra Ghana
International Institute for Multidisciplinary and Development Research
Harmath Global Educational Services

38th International Science Technology Education Arts Management
& Social Sciences (iSTEAMS) Bespoke Conference - Accra Ghana 2024

Cybersecurity and Data Privacy in Remote Work and GIG Economy

[1]Adedoyin A. Talabi & [2]Olumide O Longe
[1]Africa Centre of Excellence on Tech Enhanced Learning (ACETEL), NOUN Abuja, Nigeria
[2]Beyond Campus Innovations (BCI), Colorado State University, Colorado USA
E-mails: doyin.talabi@gmail.com; longeolumide@fulbrightmail.org
Phone: +2348033601054; +2348160900893)

ABSTRACT

The GIG economy and the shift to remote work have transformed organizational and individual approaches to work globally. While these models create flexibility and opportunities, they have also introduced new vulnerabilities around cybersecurity and data privacy. This paper investigated the cybersecurity and data protection challenges in remote work and gig-economy based employment, using a mixed-method approach that combines literature review with a survey of views from 64 professionals across different sectors. The survey findings reveal a clear and present danger in the remote and gig economy. A significant portion of the workforce use personal devices and public Wi-Fi, insufficient security tools, and lack critical, formal, frequent cybersecurity training. Recommendations include use of separate work and personal devices, workers should train regularly whether provided by the employer or not; Organizations should provide adequate resources and train workers; VPN subscriptions and password managers should be provided as standard practice, organizations should foster a shared compliance responsibility culture and strengthen security protocols that compel the use of VPN for sensitive tasks if public wi-fi networks must be used.

Keywords: Cybersecurity, Data Privacy, Remote Work, GIG Economy

Proceedings Citation Format
Adedoyin A. Talabi & Olumide O Longe (2025): Cybersecurity and Data Privacy in Remote Work and GIG Economy. Combined Proceedings of the 39th iSTEAMS Multidisciplinary Bespoke Conference 17th–19th July, 2025 & iSTEAMS Emerging Technologies Conference 30th–31st October, 2025. Ghana-Korean Information Resource Centre, Balme Library, University of Ghana, Accra, Ghana. Pp 63-72. www.isteams.net/ghana2025
dx.doi.org/10.22624/AIMS/ACCRABESPOKE2025P8

1. INTRODUCTION

The modern workplace has undergone significant transformation, accelerated by the COVID-19 pandemic and the proliferation of digital platforms. Remote work has enabled organizations to maintain productivity while reducing geographical constraints, while the gig economy has empowered workers with flexibility and new income streams.

However, both trends expose individuals and institutions to heightened cybersecurity and data privacy risks. For instance, gig workers often use personal devices with limited safeguards, while remote employees may rely on insecure home networks. In regions such as West Africa, where digital adoption is rising but governance frameworks remain inconsistent, these risks are magnified. These realities demand fresh approaches to managing risks and ensuring compliance with frameworks like the Nigeria Data Protection Act (NDPA 2023) and GDPR. This paper examined these challenges and made recommendations for individuals and organizations for a secure remote work platform and the gig economy.

1.1 Objectives

- To identify cybersecurity and data privacy risks in remote work and gig economy contexts.
- To assess awareness and practices of gig workers and remote employees.
- To recommend best practices for secure and sustainable adoption of remote work and gig economy.

1.2 Theoretical Frameworks

This paper adopted a multi-level conceptual framework combining organizational, regulatory, and individual perspectives to examine cybersecurity and data privacy challenges in remote work and the gig economy. Four complementary theories were employed:

- Agency Theory explains how conflicting incentives between organizations (principals) and remote/gig workers (agents) create risks of moral hazard and data misuse, prompting firms to adopt monitoring and control mechanisms (Jensen & Meckling, 1976).
- Institutional Theory shows how external pressures, such as laws, regulators, and stakeholder expectations drive organizations to adopt data protection practices and recognized cybersecurity standards (Meyer & Rowan, 1977; DiMaggio & Powell, 1983), including compliance with laws like the Nigeria Data Protection Act (NDPA 2023), the EU General Data Protection Regulation (GDPR), and information security standards (e.g., ISO/IEC 27001).
- Protection Motivation Theory (PMT) explains how individuals' perceptions of threat severity, vulnerability, and the effectiveness/feasibility of countermeasures influence cybersecurity behaviors (Rogers, 1975, 1983).
- Technology Acceptance Model (TAM) highlights that user acceptance of security tools depends on perceived usefulness and ease of use, helping explain adoption gaps among remote and gig workers (Davis, 1989).

Together, these theories establish a comprehensive foundation for analyzing the intersection of cybersecurity, data privacy, and evolving work arrangements in the remote work and the gig economy.

2. LITERATURE REVIEW

2.1 The Shifting Landscape of Work

According to (El-Farr, 2024), the nature of work and workplace dynamics has been transformed by the development and adoption of new technologies such as the Internet, cloud computing and artificial intelligence. The advent of COVID-19 also served to accelerate this adoption and prompted the development of new working methods and technological solutions to adapt to the challenges created by the pandemic.

This has prompted scholars to say that we have transitioned into the fourth industrial revolution and moving towards the fifth generation with the proliferation of Natural Language Processing (NLP) - based systems. Arising from the pandemic experience, many workers desired flexible work arrangements and work-life balance. As such, dependence on information and communication technologies increased and hybrid work has become the norm. Also, recent migration of skilled employees in key sectors like Information Technology, Healthcare has necessitated new working models, so that organizations can tap into global talent pool irrespective of location. However, all these has created new cybersecurity vulnerabilities and data privacy compliance challenges.

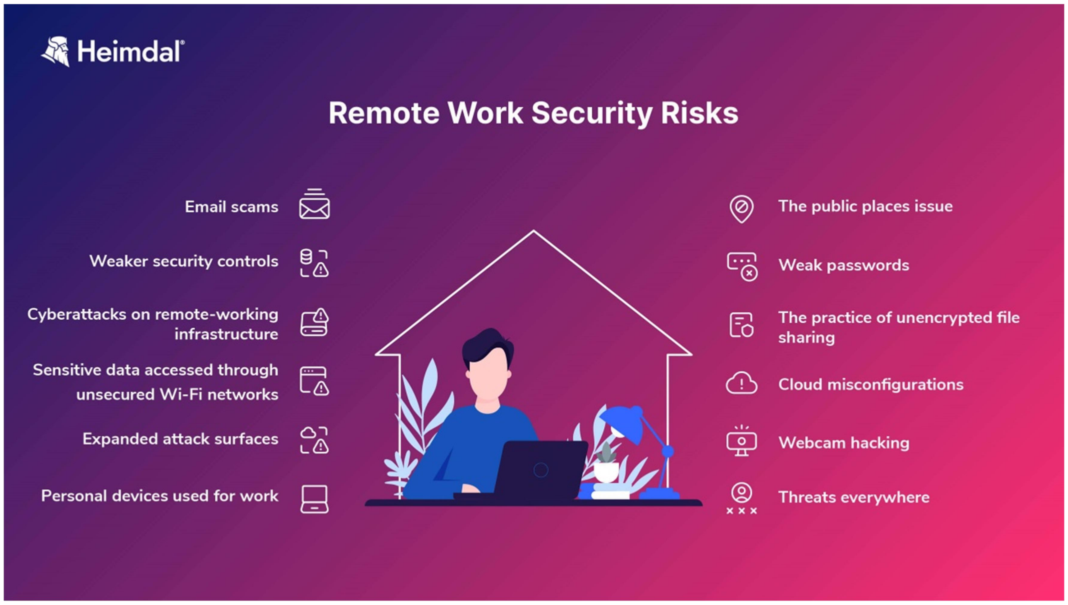
Heimdal
Remote Work Security Risks
Email scams
Weaker security controls
Cyberattacks on remote-working infrastructure
Sensitive data accessed through unsecured Wi-Fi networks
Expanded attack surfaces
Personal devices used for work
The public places issue
Weak passwords
The practice of unencrypted file sharing
Cloud misconfigurations
Webcam hacking
Threats everywhere

Fig: Remote Work Security Risks
Source: sites.psu.edu

2.2 Remote Work

Sky (2025) explained that remote work is an employment arrangement where an employee performs job duties from a location outside of a traditional corporate office, such as a home, co-working space, or cybercafé, using digital tools to collaborate with colleagues and complete tasks. Key benefits for employees include saving commuting time and costs, increased work-life balance, greater autonomy, flexible working hours, geographical freedom, access to a broader range of job opportunities and sometimes savings in external childcare costs. For employers, benefits include increased employee satisfaction and retention, potential productivity gains, and cost savings on physical office resources. However, Remote work can be fully remote (no office presence) or hybrid (a mix of office and remote work)

2.3 The Gig Economy

The gig economy refers to a labour market characterized by the prevalence of short-term contracts or freelance work, as opposed to permanent jobs but may lack benefits associated with traditional employment. This work arrangement is often facilitated by online platforms that match workers with customers for a single task or project, and is mainly done through remote work.

The gig economy has grown significantly in recent years, and its value is set to reach $873000.0 million by 2027. Some see it as a flexible and convenient way to earn income, while others view it as a manifestation of insecure work with limited benefits and protections. Nevertheless, the gig economy gives a person flexible working hours while still making a living. Examples include ride-hailing apps like Uber, food delivery apps (e.g. Glovo), holiday rental apps (Airbnb) and professional project delivery platforms (e.g. Fiverr and Upwork). With this arrangement, employees can be fully remote and work entirely from a chosen location, or have a hybrid arrangement. Also, organizations can access a broader talent pool without long-term commitment, while employees can better manage work-life balance. (aristo sourcing, 2025).

Both concepts are related but distinct: remote work is a work arrangement, while the gig economy is a labour market structure. These arrangements have challenges, such as maintaining team cohesion, loyalty and motivating a workforce that is not committed to long term goals of the organization. When businesses accidentally break labour rules and regulations due to employee misclassification, they may face legal consequences like fines and court action, which affect credibility and affect relationship with both clients and gig workers. For employees, the risks include lack of job security, unstable and inconsistent income and legal challenges to enforce their rights, benefits and limited protection against unfair practices, abuse or injuries at work (Manevska, 2025)

2.4 Cybersecurity Risks in Remote Work

Remote work security becomes very important when employees perform their tasks and access corporate resources from outside the office. These has blurred the lines between corporate and personal networks, devices, and data, extended the security perimeter and creating more entry points for attackers. Threats and risks have also increased with greater adoption of online platforms. These threats include malware, ransomware attacks, distributed denial-of-service; Camfecting, which is hacking into a webcam and activating it and zero-day exploits for which defense has not been built by developers. Risks include unsecured home networks, unpatched personal devices, weak passwords on home routers, and the use of public Wi-Fi without a Virtual Private Network (VPN); using personal devices at work (Bring-Your-Own-Devices), social engineering attacks like phishing and smishing (SMS), transferring unencrypted files, reliance on cloud services for collaboration, applications and storage of data. (Mandadi et al., 2024).

2.5 Data Privacy Risks in Remote Work

Remote work comes with many data privacy vulnerabilities arising from the use of personal devices for work, unsecured home networks, and the challenge of maintaining consistent security protocols across distributed teams. There are also risks from data loss from stolen or lost devices, improper data handling, missed communication when working in silo, employees leaving devices in public places, lack of control of how sensitive data are used, stored or deleted, endpoint security issues and difficulty in complying with data privacy rights and responsibilities in different jurisdictions. (Thorpe-Smith, 2025). Also, while many countries in Africa have data protection laws like the Nigeria Data protection Act 2023, compliance and enforcement is still weak due to infrastructure and capacity challenges.

2.6 Other Risks and Challenges in Remote Work and Gig Economy

According to (Bahu, 2024) other risks and challenges include limited career advancement and requires continued upskilling, lack traditional benefits like health insurance, paid leave and retirement plans. Psychological and social challenges include social isolation, missing out on social interactions which may lead to feelings of loneliness. Mental health can also be affected negatively by the combination of uncertainty, lack of security, and isolation.

2.7 Related Works

In a global survey of ten (10) online gig platforms which covered 17 countries, (Datta et al., 2023) found that the gig economy is growing but lacks reliable data and needs regulatory action and policies to address risks. The study identified 545 online gig work platforms across the globe. Nearly three-quarters (72.8%) of these are regional or local platforms. These local platforms play a crucial role by lowering entry barriers, adapting to local constraints, and overcoming language barriers. Local platforms also cater to local businesses, including micro, small, and medium-sized enterprises (MSMEs) and startups. While developed countries dominate the demand for online labour, the growth rate is faster in developing countries. The findings from the survey show that many are predominantly young, with most being under 30.

This presents a potential solution for countries with high youth unemployment. It also found that while men dominate the workforce, participation by women is higher in some regions compared to the general labour market and over 6 in 10 gig workers live in smaller cities and towns and for two in three workers, gig work is a secondary or sporadic occupation. Gig workers are not poor enough for social safety nets and not well-off enough for formal social insurance programs, making them vulnerable due to volatile earnings. They have limited access to health insurance and old-age pensions. The challenges to social protection for gig workers are compounded by a lack of a clear employment status, a lack of systems to cover self-employed workers, and a lack of collective bargaining power.

The paper recommended that developing countries address social protection by partnering with digital platforms for broader policy goals, supporting new models of collective bargaining, clarifying the employment status of gig workers, innovating and experimenting with social insurance designs and collecting data to track and monitor the gig worker population. In order to maximize the benefits of gig work, it is essential to build digital skills, promote labour market inclusion, enhance social protection coverage, use e-governance reforms to create new opportunities, and support the growth of local private sectors.

3. METHODOLOGY

The paper used a mixed-method approach by reviewing industry reports for qualitative analysis and for quantitative analysis used a structured 20-question questionnaire distributed among gig workers, freelancers, and remote staff that include people in IT-related roles like Hardware Management and IT Support, Data Privacy and Protection, Information Security and Consulting. Others roles included professionals in Human Resources and Administration, Risk and Compliance, Operations, Fintech, Agriculture, Energy, Education, Healthcare and Customer Experience. A survey sample of 64 respondents was drawn from the researcher's online platforms and professional networks. This approach was chosen because of time and resource constraints but still provided access to reliable individuals actively engaged in remote work and the gig economy.

While the sample size is modest, it is sufficient to highlight major patterns, generate insights, and inform future research directions. (Bujang et al., 2024; Totton et al., 2023). Questions asked related to exposure and experience with remote work ad gig economy, practices and tools used, data privacy and cybersecurity awareness and perception, and platform trust and governance issues. The survey was analyzed using descriptive statistics for quantitative data and thematic analysis for qualitative insights.

4. LIMITATIONS

This study has some limitations including the sample size of 64 respondents which limits the statistical generalizability of the findings. Secondly, participants were recruited primarily through the researcher's own online platforms and professional networks. As such, the sample may be biased to individuals who are digitally active, connected to the researcher's online groups, or share similar perspectives on remote work and the gig economy. Consequently, the results may be reflecting the experiences of this specific group rather than the broader population of remote and gig workers. Despite these limitations, the study provides valuable preliminary insights that can inform larger and more representative future research. (MindTheGraph Team, 2024; NN/g, 2025; OmniConvert, 2025)

5. FINDINGS

5.1 Findings

51.6% of respondents are in IT-related jobs include roles in Data Privacy, Data Privacy and Protection, Information Security, IT Consultant, hardware management and IT support, and IT Helpdesk. Other roles included Risk & Compliance, Finance, Operations, Consulting, CEO, Fintech, Mgt Consulting, Admin and Human Resources, Healthcare, Education Agriculture, Energy, Fashion and Customer Experience. The rest of the survey results are shown in the visual figures on the next page.

30.2% of participants receive cybersecurity training frequently from their company or clients, 27% receive occasionally, 19% rarely and 17.5% have never received any training. 1.61% are not confident they can identify phishing email, 14.52% are somewhat confident, 25.8% are confident, 32.2% are quite confident and 25.8% very confident.7.9% are not confident about securing their home wi-fi network, 12.69% are somewhat confident, 33.33% are confident, 25.39% are quite confident and 20.63% are very confident. 4.8% are not confident that they how to respond to a data breach, 22.58% are somewhat confident, 20.97% are confident, 32.25% are quite confident and 19.35% very confident that they know how to respond to a data breach 52.4% use dedicated device for work to minimize security risks while 47.6% share device between personal use and work. 74.6% have access to sensitive personal data while 25.4% do not. 76.2% are very aware of Data privacy regulations, 15.9% are somewhat aware, 6.3% are not very aware and 1.6% are not sure if the regulations apply to their work.

40.3% believe that thy have a greater responsibility for protection data privacy than their clients or employers, 35.5% believe it is a shared responsibility, 14.5% believe they have a shared responsibility and 9.7% believe their employers or clients responsibility is greater. 38.1% completely trust their employers or platform to protection their personal and work data, 36.5% have some trust, 20.6% are neutral, 3.2% have very little trust and 1.6% have no trust at all. 63.5% are very concerned about sharing their personal data with third parties, 23.8% have some concerns, 6.3% are neutral and 6.3% concerned a bit. 57.1%

believe that the shift to remote work has made individuals more vulnerable, 9.5% less vulnerable, 12.7% no change in the level of vulnerability and 20.6% are not sure

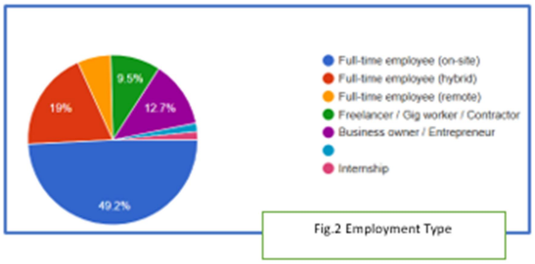

Fig.2 Employment Type

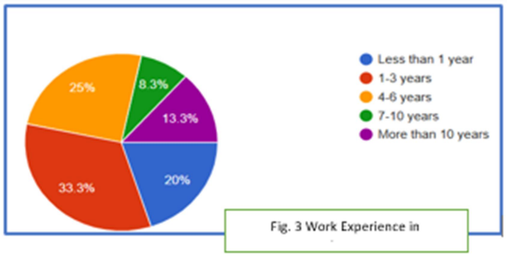

Fig. 3 Work Experience in

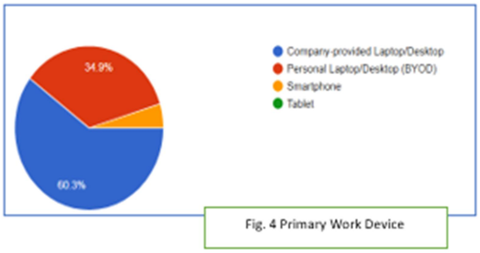

Fig. 4 Primary Work Device

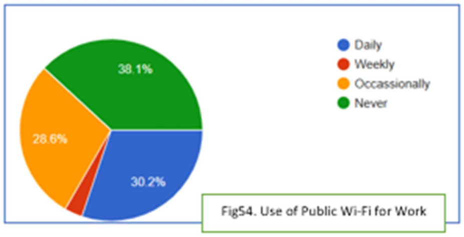

Fig54. Use of Public Wi-Fi for Work

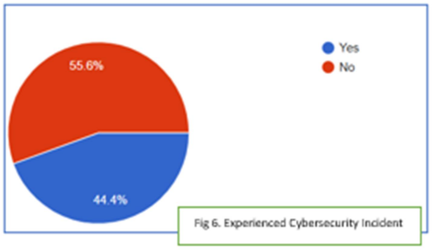

Fig 6. Experienced Cybersecurity Incident

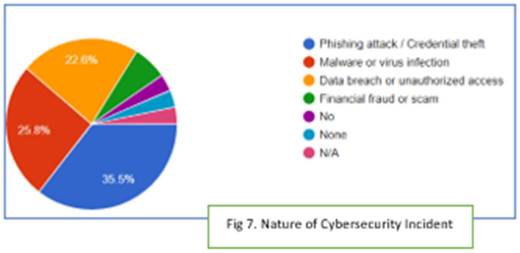

Fig 7. Nature of Cybersecurity Incident

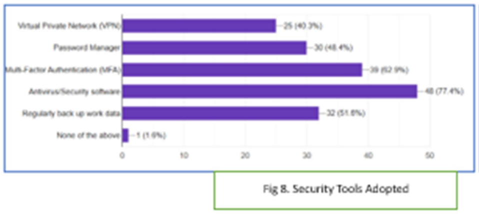

Fig 8. Security Tools Adopted

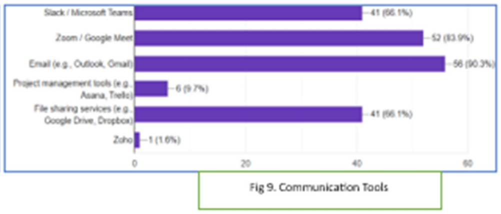

Fig 9. Communication Tools

7.2 Identified Threats and Challenges of Remote Work and Gig Economy

Respondents identified phishing and social engineering attacks as the most frequent threat, often combined with credential theft, as attackers exploit the "human factor" to gain access to accounts and data. Respondents had concerns about data compromise, data theft from unauthorized access, and data breaches are prominent. Malware, ransomware, and virus attacks were identified as significant cybersecurity threats. Many respondents highlighted the lack of cybersecurity awareness, regular sensitization, and enterprise-grade security training/tools for remote and gig workers, making them more vulnerable. Other threats included insecure home networks, unmanaged software, insufficient data encryption, and carelessness with sensitive data

7.3 Recommendations from Respondents

Respondents advised that organizations should prioritize cybersecurity awareness, workers should be trained on data privacy to understand potential vulnerabilities and mitigation. Workers should always enable multi-factor authentication (MFA) and use strong, unique passwords, ideally with a password manager. Separate personal and professional digital lives by using different email accounts, dedicated devices, or separate user profiles for work. Be cautious of sites visited, verify websites and emails to avoid phishing, refrain from downloading free software, avoid opening unsolicited emails, and be circumspect about using public Wi-Fi. Workers should use licensed software, ensure endpoints are well-protected with active antivirus software, and secure the home network, leveraging VPN technology for connectivity.

8. DISCUSSION OF FINDINGS

A diverse professional demographic is represented in the data, with a notable presence of full-time on-site employees and business owners alongside remote and gig workers. A considerable portion (33.3%) of participants are relatively new to remote or gig work, having worked in this capacity for less than three years. This demographic trend suggests that many individuals are still adapting to the unique security challenges of this work model. The widespread use of personal laptops and desktops (34.9%) and public Wi-Fi (30.2% daily use) for work-related activities stands out as a critical security risk. These practices increase the attack surface, making individuals more susceptible to data breaches and network-based threats. While a high percentage of respondents use fundamental security measures like antivirus software (77.4%), the adoption rates for other crucial tools like password managers (48.4%) and VPNs (40.3%) are notably lower.

This indicates a gap in understanding or prioritizing layered security practices. The high percentage of respondents who share devices for personal and work use (47.6%) further compounds this risk. Given that 74.6% of participants handle sensitive personal data, this lack of a dedicated work device and inconsistent tool adoption creates significant liability. The results point to a major deficiency in cybersecurity training. A substantial portion of the participants receive training only occasionally (27%), rarely (19%), or never (17.5%).

This lack of formal guidance likely contributes to the overconfidence observed in certain areas. For instance, participants express high confidence in their ability to identify phishing emails, yet 44.4% have experienced a cybersecurity incident, with phishing being the most common type of attack. This discrepancy between perceived confidence and real-world experience highlights a dangerous knowledge-practice gap. The fact that a majority of respondents believe the shift to remote work has made individuals more vulnerable, and that over 40% feel they bear the greatest responsibility for data protection, underscores the perceived lack of support from employers and a need for more robust, shared security models.

9. CONCLUSION

The survey findings reveal a clear and present danger in the remote and gig economy. A significant portion of the workforce is operating with suboptimal security practices (using personal devices and public Wi-Fi), insufficient security tools, and a critical lack of formal, frequent training.

The high rate of cyber incidents confirms that these vulnerabilities are not theoretical; they are actively being exploited. Individuals are aware of the risks and are concerned, but they lack the resources, support, or practical knowledge to effectively mitigate them. The current model places a disproportionate amount of responsibility on the individual, even when dealing with sensitive data, without providing adequate protection.

10. RECOMMENDATIONS

Individuals should separate devices for work and personal use and adopt password managers to create strong, unique passwords. Workers should seek out and get cybersecurity training, even if not provided by the employer. (Global Cyber Alliance, 2024). Organizations and platforms should provide adequate resources, training and security tools and foster a shared compliance responsibility culture among workers. They should also implement applications and policies that prevent use of public Wi-fi for essential tasks unless a VPN is used. (NIST, 2020).

REFERENCES

- Ahmed, S. K., & colleagues. (2024). How to choose a sampling technique and determine sample size. Journal of Research Methods in Social Science, https://doi.org/… (ScienceDirect–coach guidance) ScienceDirect
- Aristo Sourcing. (2025). The gig economy and remote work trend and the role of VAs. https://aristosourcing.com/the-gig-economy-and-remote-work-trend-and-the-role-of-vas/
- Bahu, A. (2024). The gig economy: challenges and advantages for employers and employees. DevelopmentAid. Retrieved from https://www.developmentaid.org/news-stream/post/183798/gig-economy-challenges-and-advantages
- Bujang, M. A., Omar, E. D., Foo, D. H. P., & Hon, Y. K. (2024). Sample size determination for conducting a pilot study to assess reliability of a questionnaire. Restorative Dentistry & Endodontics, 49(1), e3. https://doi.org/10.5395/rde.2024.49.e3 rde.ac
- Datta, N., Chen, R., Singh, S., Stinshoff, C., Iacob, N., Nigatu, N. S., ... & Klimaviciute, L. (2023). Working Without Borders: The Promise and Peril of Online Gig Work. The World Bank.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101
- El-Farr, H. (2024). Introductory Chapter: The Changing Landscape of Workplace and Workforce – An Overview. IntechOpen. doi: 10.5772/intechopen.1005326
- Global Cyber Alliance (2024). How to Protect Your Privacy When Working or Studying Remotely. https://globalcyberalliance.org/how-to-protect-your-privacy-when-working-or-studying-remotely/
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

- Mandadi, S., Gochhayat, S. P., Torremocha, V., & Kethar, J. (2024). Cybersecurity Risks in Remote Work and Learning Environments and Methods of Combating Them. Journal of Student Research, 13(2). DOI:10.47611/jsrhs.v13i2.6808
- Manevska, A. (2025). Advantages and Disadvantages of the Gig Economy. Native Teams. Retrieved from https://nativeteams.com/blog/gig-economy-advantages-and-disadvantages
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340–363. https://doi.org/10.1086/226550
- MindTheGraph Team. (2024, December 17). Convenience sampling: When and how to use this method. MindTheGraph Blog. https://mindthegraph.com/blog/convenience-sampling Mind the Graph
- National Institute of Standards and Technology. (2016). Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (NIST Special Publication 800-46 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-46r2
- NN/g (Nielsen Norman Group). (2025, April 18). Convenience vs. probability sampling in UX research. NN/g Articles. https://www.nngroup.com/articles/convenience-vs-probability-sampling/ Nielsen Norman Group
- OmniConvert. (2025, February 14). Convenience sampling explained. OmniConvert Research Hub. https://www.omniconvert.com/what-is/convenience-sampling/
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153–176). Guilford Press.
- Sky, E. (2025). What is remote work? - Meaning, benefits & more | Simpplr. Simpplr. https://www.simpplr.com/glossary/remote-work/
- Thorpe-Smith, J. (2025). Remote work security: How to mitigate data risks? Metomic. https://www.metomic.io/resource-centre/the-challenges-of-dlp-for-remote-working-and-how-to-manage-it
- Totton, N., Staniszewska, S., Barrios, J. P., & Jones, J. (2023). A review of sample sizes for UK pilot and feasibility studies. Pilot and Feasibility Studies, 9, 14. https://doi.org/10.1186/s40814-023-01416-w BioMed Central