Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 10, 2025

DIGITAL TRANSFORMATION IN PAKISTAN: CYBER-SECURITY LAWS, DIGITAL MEDIA, AND YOUTH GIG WORKERS – ASSESSING AWARENESS, VULNERABILITIES, AND ECONOMIC IMPACT (2024-25)

Dr Moneeba Iftikhar[*1], Dr. Hafsa Batool[2], Zainab Asghar[3], Shafaq Shabahat[4]

[*1]*Faculty, Mass Communication Lahore College for Women University, Lahore*
[2]*Faculty, Dept of Economics Lahore College for Women University, Lahore*
[3]*Ms Scholar Mass Communication Lahore College for Women University, Lahore*
BA-LLB Student, Lahore University of Management Sciences (LUMS), Lahore

[*1]moneeba.iftikhar@lcwu.edu.pk, [2]hafsah.batool@lcwu.edu.pk, [3]25090079@lums.edu.pk, [4]shafaqkhan807@gmail.com

[*1]https://orcid.org/0000-0001-6850-4203

DOI:https://doi.org/10.5281/zenodo.17265151

Keywords
Cybersecurity, Youth Gig Workers, Digital Transformation, Pakistan, Awareness, Economic Impact

Article History
Received: 13 August 2025
Accepted: 23 September 2025
Published: 04 October 2025

Copyright @Author

Corresponding Author: *
Dr Moneeba Iftikhar

Abstract

The rapid digital transformation in Pakistan has increased youth gig workers' reliance on technology, exposing them to cyber threats that may impact their economic well-being. This qualitative study examines the perceptions, awareness, and experiences of youth gig workers in Pakistan concerning cyber security laws, digital media, and online safety. Semi-structured interviews with 15 participants aged 20-24 from economics, IT, computer science, and commerce backgrounds actively engaged in online work and were conducted. Findings reveal that despite moderate to high cyber security awareness, gaps in safe practices persist, with risky behaviors like password sharing and clicking unknown links prevalent. Peer influence and social learning drive security behavior more than formal education. Participants acknowledged cyber threats' economic impact, but reporting rates remained low, possibly due to distrust or lack of awareness. The study proposes an inductive framework outlining relationships between internet usage, privacy practices, risk perception, and economic impact, as well as the influence of information sources, peer influence, and safety intentions on economic outcomes. Findings highlight the need for targeted education, policy enforcement, and awareness campaigns to address the awareness-action gap and safeguard youth gig workers' economic well-being in Pakistan's evolving digital landscape.

INTRODUCTION

Cybersecurity awareness is crucial for confronting the cumulative cyber challenges that are rising for involving and preparing internet-based earners (Khoo, Yatim, & Wong, 2025) since Cyber security is central worldwide and integrates implements, policies, and risk management to protect digital possessions (Alahmari & Duncan, 2020). Cybercrimes, though non-physical, threaten virtual identities dependent on technology, damaging online personas and institutions (Broadhurst, 2014). As an emerging turf (Lowry et al., 2017), research on human behavior in cyber threats is limited (Schneier,

2015). Nevertheless, cybercriminals exploit meager security conducts. Hi-tech ramparts alone are deficient (Abawajy, 2014), so more cyber security is needed in the coming times (Bulgurcu et al., 2010; Haeussinger & Kranz, 2013). Behavioral research comprises only 4% of Cybersecurity literature, mostly from developed nations (Gillam & Foster, 2020), but not found from developing side Cyber security-based research in developing countries is scarce, like in Pakistan (AlMindeel & Martins, 2020), which is paramount. Studies regarding cyber securities expose the fragility of personal identification in digital networks, with criminals exploiting hacking tools and virtual systems, making detection difficult (Alazab & Chon, 2014). For evidence from underdeveloped or developing nations, which is essential for policymakers, Efforts should prioritize tracking, prosecuting, and penalizing cybercriminals over mere prevention (Anderson et al., 2019). Traditional crimes like welfare and tax fraud have evolved into credit card fraud and digital scams. Consumers pushed to engage with the digital economy are at a greater risk of consumer fraud (Phua, Wei, & Yu, 2025). With growing ICT dependence and a youth-driven digital economy, Pakistan, under the category of a developing economy, faces increasing cyber threats due to socio-political instability ("Payoneer | The Global Gig-Economy Index: Q2 2019, 2020"; Shad, 2019). As Pakistani youth are engaged in certain earning opportunities as called Youth Gig Workers are now endanger cyber security through risky online behaviors (Aliyu et al., 2010), endangering personal and established safety (Al-Janabi & Al-Shourbaji, 2016). Cyber security, aimed at protecting digital systems and data from cyber-attacks, ensures information confidentiality, integrity, and availability (Seemma et al., 2018). In Pakistan, Youth Gig Workers highly exposed to the internet and prone to careless ICT use (Aliyu et al., 2010) become prime cybercrime targets (Jeske & Van Schaik, 2017; Mohebzada et al., 2012; Livingstone et al., 2014; Öğütçü et al., 2016). The rapid digital transformation, accelerated by the COVID-19 pandemic, has made cyber security a more critical issue due to rapid digital transformation and reliance (Akdeniz, 2023; Bilakeri & Kotegar, 2023; Debala et al., 2023; Garba et al., 2020; Hong et al., 2023; Wirawan et al., 2023). This shift raises privacy and data protection concerns, particularly in educational contexts.

In Pakistan, challenges include a lack of cyber security awareness, insufficient resources for businesses, and inadequate legal frameworks, making individuals and organizations vulnerable to cyber threats. Public misconceptions, unrealistic expectations of businesses, and a general lack of knowledge exacerbate the problem (Shea, 2022). This qualitative study explores Youth Gig Workers' perceptions of cyber security, awareness of cyber laws, and trust in Cybersecurity protections, aiming to inform strategies to enhance understanding and safeguard Pakistan's digital future. Many young adults in Pakistan lack Cybersecurity and online safety awareness, exposing them to increased risks in the digital landscape.

Objectives:

1. To examine Youth Gig Workers' awareness of Cybersecurity.
2. To explore these youngster's understanding of cyber laws.
3. To assess trust in Cybersecurity laws and protect against cyber-attacks.
4. To extract future safety measures from the minds of youth gig workers.
5. To explore the economic vulnerabilities of youth gig workers due to Cybersecurity threats.

Literature Review:

Cybersecurity awareness is the proper knowledge about digital safety, which addresses cyber information security risks (Kim et al., 2019; Bulgurcu et al., 2009). Hackers are too smart to mark individuals as peculiar, and professional lives congregate connected digitally due to extensive dependency and use of technology. Effective digital literacy and security training with precarious measures can alleviate these threats (Bulgurcu et al., 2009). Dependency on computers has fueled the rise of cybercrimes. Computers revolutionized industries, allowing engineers to simulate designs, save costs, and enable cybercrimes (Kim et al., 2019). Business, banking, and education have shifted online, increasing benefits and vulnerabilities (Hiscox, 2019). Cybercrimes, including fraud and extortion,

are harder to trace and costly to investigate (Bulgurcu et al., 2009).

Digital technology has reduced in-person interactions, with businesses and crimes moving online. Reports highlight a sharp rise in cybercrime, from $3 trillion in 2015 to $6 trillion in 2021, expedited compared to traditional crimes (Anderson et al., 2019). Cybercriminals increasingly outpace defenders, making individuals the weakest link in the security chain (Sardar & Wahsheh, 2020). A study on farmers revealed that over half had experienced cybercrimes, with perceptions shaped by gender, education, and self-efficacy in handling cyber threats (Geil et al., 2018).

Certain Muslim countries following Sharia law have adapted it to combat cybercrime (Hasanah, 2018). For example, in Saudi Arabia and the UAE, cybercrimes like tapping are punishable by physical penalties, such as amputation, which aligns cybercrimes with traditional offenses (Hashanah, 2018). These nations do not differentiate between physical and cybercrimes; they only distinguish between the methods used to commit them. The Norton Cyber Safety global survey shows evidence of increased cybercrime threats over time, with participants increasing online safety measures, although many remain unsure how to protect themselves (Symantec, 2019). The Internet of Things (IoT) provides many benefits, particularly in smart applications, but still, when it comes to security, risks are rapidly increasing, contributing to various crimes (Gurunathan et al., 2022). IoT connects billions of devices, storing and accessing data on online servers, which makes it susceptible to breaches. The growing prevalence of IoT in daily life highlights the need for increased awareness of cyber threats. A study of papers published from 2010-2019 revealed the ever-increasing focus on IoT, with half of the firms experiencing cyber-attacks, according to the 2019 Hiscox Cyber Readiness Report. Cybercriminals have been increasingly well-attached, using official narratives in an original way that helps them to facilitate crimes (Lallie et al., 2021). The COVID-19 pandemic exacerbated these risks, with online commerce and gaming becoming hotspots for cybercrime.

A significant rise in cybercrime was noted globally, with over 330 million people affected in 2019. People in Japan are particularly concerned but unsure about how to defend themselves against cybercrimes (Harris Poll, 2019). Cyber threats are diverse and challenging to track (Guinchard, 2011). Software vulnerabilities often lead to cybercrimes, making it crucial to address these gaps in Cybersecurity (Bederna & Szadeczky, 2020). Establishing cyber ethics based on universal discourse ethics is essential to countering cybercrimes like deepfakes and cyberterrorism (Mbinjama-Gamatham & Olivier, 2020; Hua & Bapna, 2013). Cyber espionage and phishing also pose significant risks to information security (Bederna & Szadeczky, 2020).

The rise in cybercrimes is associated with global digitalization, with Pakistan experiencing an 83% increase in cybercrime over the last three years (DAWN). The Prevention of Electronic Crimes Act (PECA) 2016 and the Electronic Transactions Ordinance (ETO) 2002 are key legal frameworks that address cyber threats, including e-commerce fraud, cyberterrorism, and illegal. To protect against cybercrime, individuals should secure devices with strong passwords, use security software, and download apps only from trusted sources. Use unique PINs, avoid public computers, and enable transaction alerts in banking. Social media should be protected with added security, restricting access to personal content, while secure internet connections require changing default admin settings, using strong passwords, and avoiding suspicious links.

Pakistan's cyber laws regulate digital media through key legislation. PECA 2016 criminalizes cyber offenses and allows content blocking (Government of Pakistan, 2016), with amendments in 2022 targeting "fake news" (Government of Pakistan, 2022) and 2025 establishing SMPRA for social media regulation (Government of Pakistan, 2025). The E-Safety Bill 2023 proposes mandatory platform registration, data localization, and restricted judicial reviews (Government of Pakistan, 2023). The Citizens Protection Rules 2020 enforce social media compliance with registration, data localization, and swift content removal (Government of Pakistan, 2020). The National Cyber Security Council Act 2014 aimed to create a Cybersecurity Council but has not been reacted to (Senate of Pakistan, 2014).

The National Response Center for Cybercrime (NR3C), under Pakistan's Federal Investigation Agency (FIA), is responsible for digital forensics, security audits, and investigations. Cybersecurity is vital to protect sensitive data and maintain public trust in digital infrastructure as technology dependence grows. The NR3C plays a crucial role in preventing cyberattacks and ensuring legal compliance.

The Pegasus cyber-attack 2016 targeted influential individuals by exploiting phone vulnerabilities to steal data. Other incidents, such as Pakistan Railways' system failure 2021 and phishing attempts against the National Bank of Pakistan in 2020, highlight ongoing cyber risks. Microsoft vulnerabilities and flaws in Whats App have also demonstrated how hackers exploit weaknesses, further stressing the need for regular updates and caution in public spaces.

Incidents such as the Pegasus hack highlight how our growing dependence on digital technology has fostered an environment where cybercrime is a constant threat. To effectively counter cyber threats, it is essential to implement proactive strategies, robust cyber laws, and efficient enforcement. Ensuring a secure digital space requires collaboration and heightened awareness to tackle the escalating global challenges of cybercrime. The Protection Motivation Theory (PMT), introduced by Rogers in 1975, is a well-recognized framework for understanding protective behaviors. This theory posits that human responses to threats are shaped by two cognitive evaluations: threat appraisal and coping appraisal (Ogbanufe et al., 2023; Rogers, 1975). Threat appraisal involves assessing the severity and susceptibility to potential dangers while coping appraisal examines self-efficacy, response efficacy, and the costs of adopting protective measures (Zhang et al., 2022). The result of these evaluations is protection motivation, which is defined as the intention to engage in protective actions (Boss et al., 2015; Rogers, 1975). In the realm of information security, PMT has been applied to various scenarios, such as responses to computer virus threats (Tsai et al., 2016), safeguarding passwords (Vedadi & Warkentin, 2020), and ensuring employee adherence to organizational policies (Alsaad & Al-Okaily, 2022; Ogbanufe et al., 2023; Sharma & Aparicio, 2022). Figure 1 depicts the model's structure, illustrating the connection between employees' intentions to follow information security policies and PMT factors. Gig workers provide on-demand services through digital platforms like Uber or TaskRabbit, often as independent contractors. These platforms connect workers with clients, offering flexibility in job selection and hours, while companies control branding, pricing, and client relationships, taking a commission from earnings. However, platform restrictions, such as non-circumvention clauses, limit gig workers' ability to build independent client bases, distinguishing this model from traditional freelance work (Donovan et al., 2016). Pakistan is among the top freelancing hubs, and Cybersecurity awareness helps students securely engage in digital work, contributing to economic sustainability. Pakistan's software exports reached $2.6 billion in 2022 but lag behind peer economies. Its global share grew from 0.17% in 2017 to 0.3% in 2021, showing potential for expansion. Strengthening policies, education, and tech adoption can enhance competitiveness (Arshad, Ahmad, & Manzoor) 2024. Digital literacy is the key to protection in South Asia, where youth are connected with the digital world and even use AI tools, very moderately understand their self-assessed digital proficiency, and primarily utilize digital applications (Hossain, Biswas, & Khan, 2025).in pakistaisn (Dahri et al., 2024)

Pakistan's IT and freelancing sectors in South Asia are pivotal in economic growth and digital transformation. Under government initiatives like tax incentives, foreign investment facilitation, and technology collaborations, the IT industry has significantly expanded, with projected revenues of $20 billion by 2025. Similarly, the freelancing sector has positioned Pakistan among the global leaders, with 42% of freelancers contributing to software development. With all these advancements, challenges and threats like energy shortages, inadequate infrastructure, and regulatory barriers hinder further growth(M. Shah et al., 2025). Teleworkers did not experience cyber-attacks in unprecedented volume, and the interview inquiry confirmed that cyber-attacks adapted to the vulnerabilities of teleworking and intensified during the pandemic. Swift adaptations and increased employee cyber-protection likely prevented further

damage in the time of the Coronavirus cyber crisis but did not eliminate cyber-attack(Khonde & Suresh, 2024)

In recent years, it has been seen at a high pace that many youngsters have launched startups during their studies. However, Cybersecurity ensures safe digital transactions and business growth, strengthening the economy. Due to rising unemployment, many young Pakistanis turn to digital labor platforms (M. M. Shah & Bashir, 2024), with freelancers often earning more than traditional workers. Pakistan ranks among the top countries in ICT outsourcing, generating significant revenue (M. Shah et al., 2025)driven by its large population of youth gig workers. With most freelancers having technical education, students in tertiary institutes are prime targets for cybercrimes, making Cybersecurity awareness crucial for economic sustainability. (Khan, Adil, Oduoye, Khan, & Ayyazuddin, 2024). Financial resources emerged as the most pivotal factor, highlighting the necessity of sufficient funding to combat evolving cyber risks.to the intricate dynamics shaping Cybersecurity expenditures in ASEAN enterprises, there is a critical need to comprehend the effects of risk antipathy(Rattanapong & Ayuthaya, 2025)

The ontological stance of the research:

This research is crucial for understanding the economic oscillation of cybercrimes, which have been shown to cost businesses billions annually, as rising cyber threats can disrupt industries and erode consumer confidence in digital platforms. By addressing cyber risks, this study contributes to safeguarding digital economies, fostering secure e-commerce, and sustaining growth in sectors dependent on online infrastructure (Gurunathan et al., 2022; Lallie et al., 2021).

Epistemological stance of the study

The epistemological approach of this study is centered on grasping the subjective views and real-life experiences of young gig workers concerning Cybersecurity awareness and online safety. It aims to investigate how these young individuals perceive and understand the risks linked to Cybersecurity, emphasizing their experiences and concerns about digital safety. The study also looks into their trust level in Pakistan's Cybersecurity laws and digital policies, considering how personal and demographic factors like age, education, socioeconomic status, and digital literacy influence these perceptions. By exploring these aspects, the study seeks to reveal the intricate ways in which young gig workers navigate the digital world, foresee potential threats, and tackle the evolving challenges of Cybersecurity in their everyday lives. This exploratory research takes an inquisitive approach, aiming to assess the relevance of Cybersecurity laws and digital policies to young gig workers in Pakistan. It further examines these young workers' concerns, opportunities, and lived experiences to generate insights for future digital policies and workforce strategies. This research is crucial for examining the Cybersecurity challenges faced by young gig workers in Pakistan, assessing their awareness, vulnerabilities, and the economic impact of digital threats. Understanding these factors can help bolster Cybersecurity policies, enhance digital literacy, and protect the expanding digital workforce. Given Pakistan's burgeoning yet fragile software export industry and rising cyber threats, this study aims to fortify Cybersecurity policies, safeguard youth gig workers, and boost the digital economy.

From the above discussion, the following are the research questions.

1. Are youth gig workers aware of cyber laws and cyber threats?
2. How do youth gig workers perceive cyber vulnerability?
3. Are youth gig workers interested in cyber security awareness for economic safety?
4. What is the economic impact of the current situation of gig workers related to digital resilience?

Research Design

A qualitative research approach was adopted to explore cyber security awareness in transforming digital safety (Braun & Clarke, 2006), grounded in the study's ontological and epistemological framework. A semi-structured interview was employed to investigate how Youth Gig Workers perceive and respond to cyber security threats. The sample consisted of 15 young people from economics, IT, computer sciences, and commerce, aged between 20 and 24, who serve as gigworkers, all

from Lahore, Pakistan, actively engaged in online working. Purposive sampling (Patton, 2002) was used to select individuals based on their digital presence and exposure to Cybersecurity issues, with eight males and seven females. Interviews were conducted until thematic saturation was attained. Somewhat than being sure of on a structured questionnaire, open-ended questions were used to scrutinize topics with participants' understanding of Cybersecurity threats, personal issues, cyber incidents (like hacking and malware), faith in Cybersecurity procedures and government measures, and their online safety practices and digital behaviors.

Findings

After interviewing these young gig workers, we have found some grounded insights into emerging themes regarding **Digital Work Habits**. What is their level of perception regarding **Cybersecurity information and experiences**? Then, later on, what are the information sources from where they **get or do not have? Then, their adaptive behavior, risk** anticipation, and action of reporting issues that can harm their monetary earning were also scrutinized. After extracting the data, some emergent relationships were also examined.

- Work Patterns & Threat Exposure → Shape Awareness
- **Peer Influence & Social Learning** → Drive Security Behavior
- **Adaptation** → Regulates Risk Reaction and reporting action.

The obtained data was transcribed and exported into NVivo 14 for data analysis. As reflected in the tables, key themes, such as patterns and words, were extracted through systematic coding until data saturation was reached. Furthermore, some new and unpredicted concepts also transpired during the analysis, contributing valued acumens to the study. The analysis is mentioned in Table 1, which contains the Inductive Framework: Cybersecurity Awareness and Practices among Youth Gig Workers.

Table 1

Cybersecurity Awareness and Practices among Youth Gig Workers

Statement	Percentage	Description	Key Quotes
1. Internet Usage Patterns			
Uses the internet for more than 5 hours daily	57.7%	It reflects heavy internet dependency among young gig workers, increasing cyber risk exposure.	"I cannot imagine a day without being online."
2. Awareness and Training in Cybersecurity			
Has moderate to high Cybersecurity Awareness	73.2%	Indicates Youth Gig Workers' general awareness, but gaps in safe practices persist.	"I know about threats, but I still take risks."
Has received formal education in Cybersecurity	60.7%	Highlights gaps in structured Cybersecurity education for Youth Gig Workers.	"Schools should teach Cybersecurity as a core subject."
3. Identification and Experience with Cyber Threats			
Can identify common cyber threats	53.2%	Suggests half of Youth Gig Workers recognize	"I can spot phishing emails easily now."

		risks.	
Has personally encountered a cyber-threat	56.7%	Nearly half of Youth Gig Workers report firsthand threat exposure.	"My social media was hacked last year."
4. Sources of Cybersecurity Information			
Relies on social media for Cybersecurity Awareness	67.2%	Social media dominates as a source for Youth Gig Workers, raising reliability concerns.	"I follow Cybersecurity pages on Instagram."
5. Privacy and Security Practices			
Concerned about personal information being shared	54.3%	Moderate concern over privacy risks among Youth Gig Workers.	"I worry about my data being misused."
Updates passwords regularly	50.3%	Half neglect password updates, indicating lax security habits.	"I use the same password for years."
Uses strong passwords and keeps them confidential	52.2%	The majority of Youth Gig Workers do not follow strong password practices.	"I use my pet's name as my password."
Uses two-factor authentication	50.3%	Even split in the adoption of enhanced security measures.	"Two-factor authentication is a hassle."
6. Cybersecurity Behavior and Practices			
Has shared passwords with someone else	56.2%	Risky password-sharing practices are prevalent among Youth Gig Workers.	"I trust my best friend with my Netflix login."
Clicks links/downloads from unknown sources	58.7%	High engagement in risky online behavior.	"I clicked a link and lost my Instagram."
Friends' behavior influences online safety practices.	60.0%	Peer influence shapes Youth Gig Workers' Cybersecurity habits.	"My friend's hacking made me more careful."
7. Reporting Cybersecurity Incidents			
Has reported a Cybersecurity incident to authorities	79.2%	Low reporting rates, possibly due to distrust or lack of awareness.	"I did not know where to report."
8. Cybersecurity Risk Perception			
Feels vulnerable to cyber-attacks	52.8%	Nearly half of Youth Gig Workers perceive personal risk.	"I feel like my data is exposed."
Believes young people are more at risk of cyber-attacks	63.7%	Strong perception of Youth Gig Workers' vulnerability.	"Teenagers share too much online."

9. Interest in understanding Cybersecurity laws			
Interested in attending Cybersecurity law workshops	50.2%	Divided interest in further education among Youth Gig Workers.	"I would attend a workshop if engaging."
10. Cybersecurity Awareness for Youth Gig Workers Ensuring Economic Safety			
Likely to improve online safety for economic safety	60.7%	**A positive willingness to embrace safer methods for secure digital income**	**"I intend to activate two-factor authentication to safeguard my online earnings."**

Visual Flow

This model is grounded in practical experiences, prioritizing adaptive learning over formal instruction in shaping Cybersecurity behaviors. The Inductive Framework is depicted as a figure illustrating how Cybersecurity awareness and practices develop through experience, peer influence, and adaptation rather than relying on predefined predictors if any adjustments are necessary

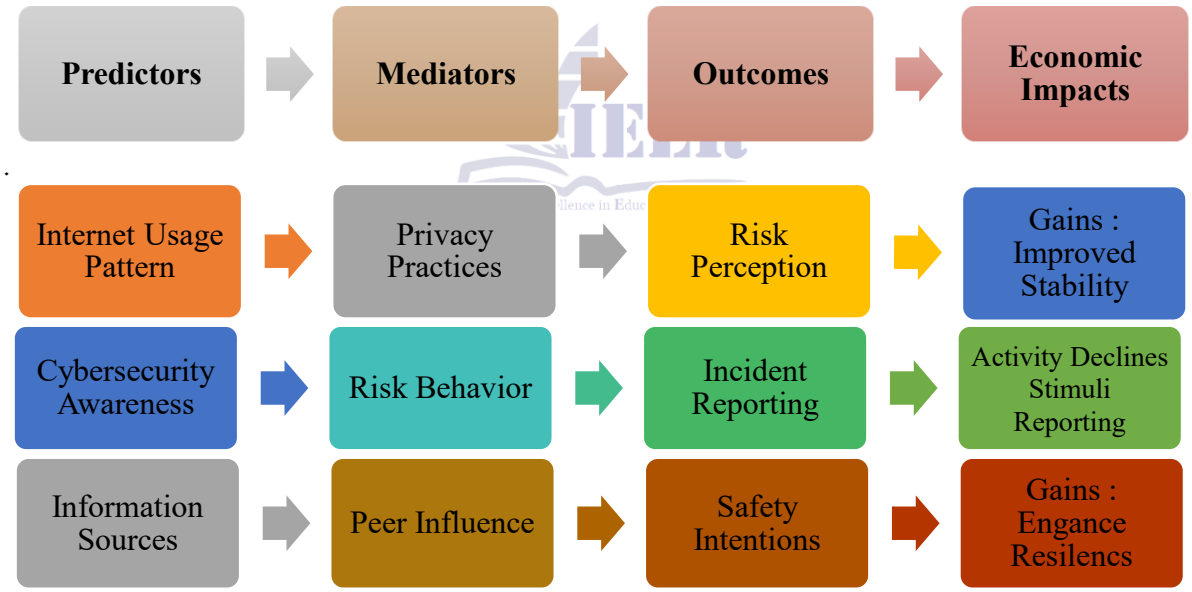


Figure 1

1. **Internet Usage → Privacy Practices → Risk Perception → Economic Impact:** Excessive internet use impacts privacy, risk perception, and, foremost mo, monetary losses.
2. **Cybersecurity Awareness → Risk Behavior → Incident Reporting → Economic Impact:** Understanding Cybersecurity leads to risk-related actions, progressing to incident reporting and resulting in efficiency losses.

3. **Information Sources → Peer Influence → Safety Intentions → Economic Impact**: Information influences peer pressure, affecting security goals and leading to long-term changes.

Discussion

This research is crucial in Pakistan's current scenario, where digital transformation is rapid. Pakistan's evolving technology terrain and youth are engaged in online earning; gig workers are engaging to navigate the challenges and opportunities presented by the economy and digital platforms shaping their future (Tariq, 2024).

1. Are youth gig workers aware of cyber laws and cyber threats?
2. Do youth gig workers perceive the risk while working?
3. How do youth gig workers perceive cyber vulnerability?
4. Are youth gig workers interested in cyber security education for economic safety?
5. What is the economic impact of the current situation of gig workers related to cyber resilience?

Studies indicate that the majority of Pakistani young gig workers are so dependent upon digital media that they feel that they cannot survive a single day without the internet, which is found common in current literature in many studies across the globe. At the same time, Pakistani youth gig workers are worried about cybercrimes, too. They are cautious regarding high levels of cyber security awareness, which aligns with studies highlighting the significance of awareness in reducing risks in previous studies (Kim et al., 2019; Bulgurcu et al., 2009). However, knowing all threats practically, even so, there are still shortcomings in safe practices, such as sharing passwords, which sounds uncanny as if they do not overhaul for this intimidation. Individuals continue to be the most vulnerable aspect of cyber security, echoing the previous findings from earlier literature (Sardar & Wahsheh, 2020). The intent to adopt safer practices (e.g., enabling two-factor authentication) was also extracted, which reflects the literature's emphasis on proactive measures to safeguard digital economies. The trivial awareness of Cybersecurity laws and divided interest in Cybersecurity education among Youth Gig Workers in Pakistan differ from previous studies that encourage robust legal frameworks and education to counter cybercrime (Hashanah, 2018; Hiscox, 2019). As the literature highlights, this gap underscores the basics of policy action and awareness campaigns.

The finding that peers' online behavior influences 60% of youth gig workers supports previous findings that view social ebbing as shaping Cybersecurity practices. Therefore, a social action and conscious call for action must be implemented to enhance it as social responsibility aligns with it (Geil et al., 2018). However, the high commitment to risky behaviors (e.g., clicking on unidentified links) is dissimilar to the literature's call for stricter adherence to secure practices (Bulgurcu et al., 2009). Moreover, a collective effort is important to make youth conscious of this.

A moderate thought of digital tools among youth gig workers reflects a balanced approach towards technology use for work. This outlook aligns with existing scholarships that allow practical engagement without overdependence on digital platforms common in the South Asian tapestry. It stresses the necessity for complete education to augment perilous appointments with technology (LIS study). While 73.2% of young gig Workers are conscious of Cybersecurity dangers, which is concocting to found, various are still involved in insecure performance, conflicting with education linking awareness to behavioral change (Bulgurcu et al., 2009; Khoo, 2025). Findings also reveal that very low reporting rates (79.2% did not report cases) contradict previous findings (Anderson et al., 2019). Unlike Muslim countries that apply Sharia law to cybercrimes (Hashanah, 2018), Pakistan's Youth Gig Workers show limited awareness of local Cybersecurity laws (e.g., PECA 2016), highlighting a gap in legal education and enforcement. While the literature emphasizes the growing risks of IoT and smart devices (Gurunathan et al., 2022), your study does not explicitly explore IoT-related vulnerabilities among Youth Gig Workers, suggesting a potential area for future research.

Conclusions

This research is crucial as an exploratory study in this era, where Pakistan is embarking on a new digital

transformation journey. It opens new horizons for future quantitative, deductive studies exploring solutions to this phenomenon. The exploratory study emphasizes that young gig workers in Pakistan spend significant time online due to their job requirements, heightening their vulnerability to cyber threats and crimes. Despite their educational qualifications, many are not well-informed about Cybersecurity laws and the risks they encounter. Issues like password sharing and transferring digital accounts are significant, often resulting in financial losses from hacking. Although the Pakistani government has established clear cybersecurity regulations, gig workers lack awareness of and interest in these legal protections. They recognize the impact of cybercrimes on their income but prioritize financial stability over understanding legal solutions. This study highlights the urgent need for strategic communication and educational efforts to raise gig workers' awareness of Cybersecurity laws. Stakeholders, including policymakers, digital platforms, and educational institutions, must collaborate to implement structured awareness campaigns. Providing gig workers with essential legal knowledge and digital security practices can protect and enhance their contributions to Pakistan's economy. The study also proposes an inductive framework that outlines Cybersecurity awareness and practices, incorporating emerging constructs relevant to this field. This framework can serve as a basis for future empirical testing, as it identifies key variables and relationships within the Cybersecurity domain for gig workers. By validating these constructs through further research, this study paves the way for developing effective strategies and interventions to improve digital security awareness and resilience among gig workers in Pakistan.

Limitations

1. The study was limited to Lahore, which has a strong digital infrastructure; results may not differ from those in underdeveloped areas like Balochistan, where internet access is poor.
2. The research sample focused on individuals from computer sciences, IT, and economics backgrounds who are more digitally aware, excluding gig workers from non-technical or less-educated segments.
3. The challenges and digital resilience of gig workers in rural or low-resource areas remain unexplored, which could lead to different findings.

Recommendations

1. Future studies should cover gig workers from underdeveloped regions and rural areas of Pakistan to understand their specific challenges.
2. Quantitative, large-scale studies are needed to measure digital resilience and coping strategies across diverse educational and professional backgrounds.
3. Policymakers and researchers should focus on improving digital literacy and infrastructure in less-developed areas, ensuring inclusive digital growth and equal opportunities for all gig workers.
4. Nonetheless, the gap between awareness and action, low reporting rates, and limited legal knowledge among Youth Gig Workers highlight areas where Pakistan's situation diverges from global patterns.
5. It is essential to address these issues through focused education, policy enforcement, and awareness initiatives to protect the economic interests of Youth Gig Workers and promote a secure digital environment.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behavior & Information Technology, 33*(3), 237–248.

Abawajy, J. H. (2014). User behavior and Cybersecurity. *Journal of Information Security and Applications, 19*, 1–13.

Akdeniz, Y. (2016). *Internet child pornography and the law: National and international responses.* Routledge. https://doi.org/10.4324/9781315581580

Alahmari, S., & Duncan, B. (2020). Cybersecurity: A review of the literature. *Journal of Cybersecurity,* 6(1), 1–22. https://doi.org/10.1093/cybsec/tyaa001

Alazab, A., & Chon, K. (2014). Cybercrime and Cybersecurity in the Asia-Pacific region. *Journal of Information Security and Applications, 19*, 1–13.

Aliyu, A., Ahmad, A., & Basir, N. (2010). Phishing attacks and countermeasures: Implications for information security and public policy. In *Proceedings of the 2010 International Conference on Information Society (i-Society)* (pp. 452–457).

Aliyu, M., Abdullah, A., & Mahmod, S. (2010). Cybersecurity awareness among students in higher learning institutions in Nigeria. *Journal of Information Security and Applications, 15*, 1–12.

Al-Janabi, A., & Al-Shourbaji, I. (2016). Cybersecurity awareness among university students in Jordan. *Journal of Information Security and Applications, 21*, 1–12.

AlMindeel, A., & Martins, J. (2020). Cybersecurity behavior in developing countries: A systematic review. *Journal of Cybersecurity, 6*(1), 1–18.

Alsaad, A., & Al-Okaily, M. (2022). Acceptance of protection technology in a time of fear: the case of COVID-19 exposure detection apps. *Information Technology & People*, *35*(3), 1116-1135.

Anderson, R., Barton, C., Böhme, R., Clayton, R., & van Eeten, M. (2019). Measuring the cost of cybercrime. *Journal of Cybersecurity, 5*(1), 1–23.

Arshad, N., Ahmad, W., & Manzoor, K. (n.d.). Unleashing the potential of Pakistan's IT industry: Building for massive software export growth. *Pakistan Institute of Development Economics Working Papers.*

Baddeley, A. (2006). Working memory. In S. Pickering (Ed.), *Working memory and education* (pp. 1–31). Elsevier. https://doi.org/10.1016/b978-012554465-8/50003-x

Baddeley, A. D., & Hitch, G. J. (2019). The phonological loop as a buffer store: An update. *Cortex, 112*, 91–106. https://doi.org/10.1016/j.cortex.2018.05.015

Bederna, A., & Szadeczky, N. (2020). Cyber threats and ethics: A systematic review. *Journal of Business Ethics, 211*(2), 347–362.

Bederna, Z., & Szadeczky, T. (2020). Cyber espionage through botnets. *Security Journal, 33*(1), 43–62. https://doi.org/10.1057/s41284-019-00194-6

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Broadhurst, R. (2014). Cybercrime and digital forensics in Asia. *Journal of Digital Forensics, Security and Law, 9*(2), 1–12.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Information security policy compliance: An empirical study of rational choice theory. *Decision Support Systems, 48*(4), 635–647.

Çeliköz, N., Erisen, Y., & Sahin, M. (2019). Cognitive learning theories emphasize latent learning, Gestalt, and information processing theories. *Journal of Educational and Instructional Studies in the World, 9*(3).

Dahri, N. A., Yahaya, N., Al-Rahmi, W. M., Vighio, M. S., Alblehai, F., Soomro, R. B., & Shutaleva, A. (2024). Investigating AI-based academic support acceptance and its impact on students' performance in Malaysian and Pakistani higher education institutions. *Education and Information Technologies, 29*(14), 18695–18744. https://doi.org/10.1007/s10639-024-12599-x

Davis, F. (2017). Promoting Cybersecurity awareness and education among youth. *Journal of Cybersecurity Policy, 2*(1), 1–20. https://doi.org/10.1007/s42438-017-0002-6

Donovan, S. A., Bradley, D. H., & Shimabukuru, J. O. (2016). What does the gig economy mean for workers? *Congressional Research Service.* https://crsreports.congress.gov

Geil, B., Hubbard, D., & Miller, R. (2018). Cybersecurity and the agriculture industry:

An exploratory study. *Journal of Agricultural and Environmental Ethics, 29*(3), 347–362.

Gillam, S., & Foster, S. (2020). Cybersecurity behaviour: A systematic review. *Journal of Cybersecurity, 6*(1), 1–18.

Goldstein, E. B., & Mackewn, A. (2005). *Cognitive psychology: Connecting mind, research, and everyday experience.* Belmont, CA: Thomson Wadsworth.

Government of Pakistan. (2016). The Prevention of Electronic Crimes Act, 2016. *National Assembly of Pakistan.* https://www.na.gov.pk/uploads/documents/1470910659_707.pdf

Government of Pakistan. (2020). Citizens Protection (Against Online Harm) Rules, 2020. *Ministry of IT & Telecommunication.* https://moitt.gov.pk

Government of Pakistan. (2022). PECA Amendment Ordinance, 2022. *Ministry of IT & Telecommunication.* https://moitt.gov.pk

Government of Pakistan. (2023). E-Safety Bill, 2023. *Ministry of IT & Telecommunication.* https://moitt.gov.pk

Government of Pakistan. (2025). PECA Amendment Act, 2025. *Ministry of Law & Justice.*

Guinchard, A. (2011). The EU online consumer: Re-booting consumer confidence in cross-border online goods shopping. *Journal of Consumer Policy, 34*(4), 447–462.

Gurunathan, R., Rajendran, L., & Kumar, M. (2022). A comprehensive survey on security and privacy issues in cloud computing. *Journal of Network and Computer Applications, 200*, 103281.

Haeussinger, F., & Kranz, J. (2013). Information security awareness: A review of the literature. *Journal of Information Security and Applications, 18*, 1–15.

Hann, I., Hui, K., Lee, S. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13–42. https://doi.org/10.2753/MIS0742-1222240202

Hasanah, H. (2018). Cybersecurity awareness among university students: A case study. *Journal of Information Security, 9*(3), 123–130.

Hiscox. (2019). *Hiscox Cyber Readiness Report 2019.* Hiscox Ltd. Retrieved February 20, 2025, from https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

Hossain, Z., Biswas, M. S., & Khan, G. (2025). AI literacy of library and information science students: A study of Bangladesh, India, and Pakistan. *Journal of Librarianship and Information Science.* https://doi.org/10.1177/09610006241309323

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *Journal of Strategic Information Systems, 22*(2), 175–186. https://doi.org/10.1016/j.jsis.2012.10.004

Jeske, D., & Van Schaik, P. (2017). Familiarity with internet threats: Beyond awareness. *Computers & Security, 66*, 129–141.

Khoo, L. J., Yatim, M. H. M., & Wong, Y. S. (2025). Research on Capture the Flag Exercises for Cybersecurity Skill Training Among Malaysian Undergraduates. *Journal of Human-Centered Technology, 4*(1), 1-9. doi:https://doi.org/10.11113/humentech.v4n1.87

Khan, Z., Adil, T., Oduoye, M. O., Khan, B. S., & Ayyazuddin, M. (2024). Assessing the knowledge, attitude, and perception of Extended Reality (XR) technology in Pakistan's healthcare community in an era of artificial intelligence. *Frontiers in Medicine, 11*, 1456017. https://doi.org/10.3389/fmed.2024.1456017

Khonde, S. M., & Suresh, L. (2024). Globalization and the evolution of labor: Navigating new frontiers in the global economy. *The Scientific Temper, 15*(4), 3369–3376. https://doi.org/10.58414/SCIENTIFICTEMPER.2024.15.4.47

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248.

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). *In their own words: What bothers children online?* European Commission Safer Internet Plus Programme.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organizational information security policies: An empirical study of the influence of counterfactual reasoning and organizational trust. *Information Systems Journal*, *25*(3), 193–273.

Mbinjama-Gamatham, A., & Olivier, B. (2020). 'Dark technology,' aggressiveness and the question of cyber-ethics. *Acta Academica, 52*(1), 99–120. https://doi.org/10.18820/24150479/aa52i1/1

Mohebzada, J. G., El Zarka, A., Bhojani, A. H., & Darwish, A. (2012, March). Phishing in a university community: Two large-scale phishing experiments. In *2012 International Conference on Innovations in Information Technology (IIT)* (pp. 249–254). IEEE.

Ogbanufe, O., Kim, D. J., & Spears, J. L. (2023). Information security compliance: The role of protection motivation theory. *International Journal of Information Management, 47*, 227–235.

Phua, K., Wei, C., & Yu, G. Y. (2025). The digital economy and consumer fraud. *SSRN*. https://doi.org/10.2139/ssrn.5137239

Rattanapong, P., & Ayuthaya, S. (2025). Influential factors of Cybersecurity investment: A quantitative SEM analysis. *Management Science Letters, 15*(1), 31–44.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114.

Senate of Pakistan. (2014). National Cyber Security Council Bill, 2014. https://www.senate.gov.pk

Shah, M. M., & Bashir, A. (2024). Investigating clickbait strategies: A CDA of Pakistani YouTube news channels. *Pakistan Social Sciences Review, 8*(2), 253–268. https://doi.org/10.35484/pssr.2024(8-II)22

Shah, M., Abbas, A., Ahmad, F., Khan, S., Khan, J., & Islam, M. (2025). Analyzing policies and practices shaping IT exports and freelancing economic impact on Pakistan. *Khyber Journal of Public Policy, 4*(1).

Sharma, R., & Aparicio, M. (2022). Compliance with organizational security policies: A study of protective motivation. *Journal of Organizational Security, 16*(1), 70–85.

Tariq, S. (2024). *Unleashing Digital Dreams: Pakistan's Gig Economy* (Doctoral dissertation, School of Social Sciences & Humanities (S3H), NUST).

Tsai, C., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Exploring users' protection behavior against computer virus threats: An empirical study based on protection motivation theory. *Computers in Human Behavior, 59*, 178–189.

Vedadi, A., Warkentin, M., Straub, D. W., & Shropshire, J. (2024). Fostering information security compliance as organizational citizenship behavior. *Information & Management, 61*(5), Article 103968. https://doi.org/10.1016/j.im.2024.103968

Zhang, W., Xiong, S., Zheng, Y., & Wu, J. (2022). Response efficacy and self-efficacy mediated the relationship between perceived threat and psychic anxiety among college students in the early stage of the COVID-19 pandemic. *International journal of environmental research and public health*, *19*(5), 2832.