साइबर सुरक्षा और आधुनिक समाज: अवसर एवं चुनौतियाँ

लेखक (Authors):
डॉ. नंदन कुमार ठाकुर[1]*, हेमंत कश्यप[2]

[1] एसोसिएट प्रोफेसर, चितकारा स्कूल ऑफ साइकोलॉजी एंड काउंसलिंग, Chitkara University, पंजाब, भारत
[2] पीएच.डी. शोधार्थी, क्लिनिकल मनोविज्ञान विभाग, Mizoram University, आइजोल, मिजोरम, भारत

संबद्धता (Affiliation):
चितकारा स्कूल ऑफ साइकोलॉजी एंड काउंसलिंग, चितकारा यूनिवर्सिटी, पंजाब, भारत

पत्राचार लेखक (Corresponding Author):
डॉ. नंदन कुमार ठाकुर
ईमेल: nandan.thakur@chitkara.edu.in
मोबाइल: 9113314960

लेखकों के ORCID:
https://orcid.org/0009-0009-2071-8064[1]
https://orcid.org/0009-0007-0448-4582[2]

सारांश

वर्तमान सूचना क्रांति के युग में मानव समाज एक तीव्र डिजिटल रूपांतरण से गुजर रहा है, जहाँ इंटरनेट और संचार तकनीकों ने शिक्षा, प्रशासन, स्वास्थ्य और सामाजिक संवाद के स्वरूप को मौलिक रूप से बदल दिया है। आज का समाज एक 'डिजिटल समाज' के रूप में विकसित हो चुका है, जहाँ सूचना का प्रवाह पारंपरिक भौगोलिक सीमाओं से परे जा चुका है। प्रस्तुत शोध पत्र सामाजिक विज्ञान के दृष्टिकोण से आधुनिक समाज में साइबर सुरक्षा के बहुआयामी प्रभावों का विश्लेषण करता है। शोध पद्धति के रूप में इसमें वर्णात्मक और विश्लेषणात्मक दृष्टिकोण अपनाया गया है, जो प्राथमिक रूप से द्वितीयक आँकड़ों जैसे NCRB (2023), ट्राई (2024) और CERT-In रिपोर्ट पर आधारित है। अध्ययन की गहराई हेतु राजस्थान और दिल्ली/NCR क्षेत्र में विश्वविद्यालयी छात्रों पर किए गए हालिया सर्वेक्षणों (2023-2025) को आधार बनाया गया है। शोध के परिणाम दर्शाते हैं कि जहाँ डिजिटल इंडिया जैसे अभियानों ने आर्थिक समावेशन और ई-गवर्नेंस के माध्यम से नए अवसर पैदा किए हैं, वहीं साइबर खतरों की जटिलता में भी अभूतपूर्व वृद्धि हुई है। NCRB की रिपोर्ट के अनुसार, वर्ष 2023 में साइबर अपराधों में 31.2% की वृद्धि दर्ज की गई, जिनमें अधिकांश मामले वित्तीय धोखाधड़ी से संबंधित थे। क्षेत्रीय अध्ययनों से यह स्पष्ट हुआ कि युवाओं में डिजिटल जुड़ाव तो उच्च है, किंतु साइबर सुरक्षा

संबंधी व्यावहारिक ज्ञान और 'डिजिटल नैतिकता' का अभाव है । लगभग 84% विश्वविद्यालयी छात्रों ने साइबर सुरक्षा को अनिवार्य पाठ्यक्रम में शामिल करने की आवश्यकता पर बल दिया है । लेख यह निष्कर्ष निकालता है कि साइबर सुरक्षा केवल एक तकनीकी समस्या नहीं, बल्कि एक साझा सामाजिक जिम्मेदारी है । एक सुरक्षित डिजिटल समाज के निर्माण हेतु 'क्रेडिट-बेस्ड' अनिवार्य साइबर शिक्षा, कड़े कानूनी क्रियान्वयन और व्यक्तिगत 'साइबर हाइजीन' के समन्वय की तत्काल आवश्यकता है ।

विशिष्ट शब्द: साइबर सुरक्षा, डिजिटल समाज, डिजिटल साक्षरता, साइबर अपराध, NCRB, डिजिटल नागरिकता, भारत ।

1. प्रस्तावना - डिजिटल युग में सामाजिक परिदृश्य का परिवर्तन

वर्तमान युग में मानव समाज एक तीव्र सूचना क्रांति (Information Revolution) के दौर से गुजर रहा है। इंटरनेट और डिजिटल तकनीक ने न केवल संचार और व्यापार के स्वरूप को बदला है, बल्कि शिक्षा, प्रशासन, स्वास्थ्य, और सामाजिक जीवन तक को गहराई से प्रभावित किया है। आज का समाज एक डिजिटल समाज (Digital Society) के रूप में विकसित हो चुका है, जहाँ सूचना का प्रवाह पारंपरिक सीमाओं से परे जा चुका है। मोबाइल एप्लिकेशन, ऑनलाइन बैंकिंग, सोशल मीडिया और ई-गवर्नेंस जैसी प्रणालियों ने मानव जीवन को अधिक सुगम और त्वरित बनाया है। किंतु इस तीव्र डिजिटलीकरण के साथ-साथ नए खतरों का भी उदय हुआ है, जिनमें सबसे प्रमुख है - साइबर सुरक्षा (Cyber Security)।

साइबर सुरक्षा का अर्थ केवल कंप्यूटर या नेटवर्क की तकनीकी सुरक्षा से नहीं है, बल्कि यह उस संपूर्ण व्यवस्था से संबंधित है जो व्यक्ति, संस्था या समाज के डिजिटल डेटा, निजता और ऑनलाइन व्यवहार की रक्षा करती है। जैसा कि Barbhuiya (2024) ने उल्लेख किया है, साइबर सुरक्षा एक बहुआयामी संकल्पना है, जिसमें तकनीकी उपायों के साथ-साथ सामाजिक और नैतिक जिम्मेदारियाँ भी शामिल हैं। यह न केवल साइबर अपराधों से बचाव का माध्यम है, बल्कि डिजिटल विश्वास (digital trust) की नींव भी है, जिसके अभाव में समाज का डिजिटल ढांचा अस्थिर हो सकता है। भारत जैसे देश में जहाँ डिजिटल क्रांति ने ग्रामीण क्षेत्रों तक पहुँच बना ली है, वहीं साइबर खतरों की जटिलता भी तेजी से बढ़ रही है। नेशनल क्राइम रिकार्ड्स ब्यूरो (NCRB) की रिपोर्ट (मनराल, 2025) के अनुसार, वर्ष 2023 में भारत में साइबर अपराध के मामलों में 31.2% की वृद्धि दर्ज की गई, जिसमें अधिकतर मामले आर्थिक धोखाधड़ी से जुड़े थे। यह स्थिति इस बात का संकेत देती है कि तकनीकी विकास के साथ-साथ

डिजिटल सुरक्षा और नागरिक जागरूकता पर भी उतना ही ध्यान देना आवश्यक है। सामाजिक दृष्टि से साइबर सुरक्षा का महत्व इसलिए और बढ़ जाता है क्योंकि यह व्यक्ति की निजता, स्वतंत्रता और सामाजिक विश्वास से जुड़ी है। उदाहरणार्थ, सुहल्का और राजपूत (2025) के अध्ययन में पाया गया कि राजस्थान के विश्वविद्यालय छात्रों में डिजिटल साक्षरता का स्तर उच्च है, परंतु साइबर सुरक्षा संबंधी व्यावहारिक ज्ञान सीमित है। यह अंतर बताता है कि तकनीकी पहुँच बढ़ने के बावजूद सुरक्षा-संवेदनशीलता में अभी सुधार की आवश्यकता है। अतः यह लेख "साइबर सुरक्षा और आधुनिक समाज" विषय को सामाजिक विज्ञान के दृष्टिकोण से समझने का प्रयास करता है। इसका उद्देश्य यह विश्लेषण करना है कि डिजिटल समाज में सुरक्षा किस प्रकार अवसर और चुनौतियाँ दोनों प्रस्तुत करती है, और नागरिक चेतना तथा नीतिगत पहल के माध्यम से एक सुरक्षित डिजिटल समाज (Safe Digital Society) कैसे निर्मित किया जा सकता है।

1.1. आधुनिक समाज और डिजिटल निर्भरता - लाभों का तुलनात्मक आकलन

वर्तमान समय में समाज का लगभग प्रत्येक क्षेत्र डिजिटल प्रौद्योगिकी (Digital Technology) पर निर्भर हो चुका है। आज बैंकिंग से लेकर शिक्षा, स्वास्थ्य, शासन और मनोरंजन — हर क्षेत्र में डिजिटल माध्यमों ने मानव जीवन को नई गति प्रदान की है। ऑनलाइन बैंकिंग ने आर्थिक लेन-देन को सरल और त्वरित बनाया है, वहीं डिजिटल शिक्षा ने भौगोलिक सीमाओं को लांघते हुए ज्ञान की पहुँच हर कोने तक सुनिश्चित की है। स्वास्थ्य सेवाओं में टेली-मेडिसिन और ऑनलाइन परामर्श ने दूरस्थ इलाकों के लोगों को चिकित्सा सुविधा से जोड़ा है। इसी प्रकार, ई-गवर्नेंस और डिजिटल पोर्टल्स ने सरकारी सेवाओं को पारदर्शी और सुलभ बनाया है (बारभुइया, 2024)।

भारत में डिजिटल इंडिया अभियान ने इस परिवर्तन को व्यापक स्तर पर आगे बढ़ाया है। पंजानी एवं मुद्गल (2025) के अध्ययन में यह पाया गया कि स्कूल और कॉलेज स्तर पर छात्रों में इंटरनेट उपयोग लगभग सर्वव्यापी हो गया है, चाहे वह शिक्षा के लिए हो या सामाजिक संपर्क के लिए। इस प्रकार, समाज के लगभग हर वर्ग — विद्यार्थी, व्यापारी, किसान, गृहिणी या वरिष्ठ नागरिक — किसी न किसी रूप में ऑनलाइन सक्रिय हो चुके हैं। इस बढ़ती ऑनलाइन सक्रियता (Online Engagement) ने "डिजिटल नागरिकता (Digital Citizenship)" की एक नई अवधारणा को जन्म दिया है, जिसमें प्रत्येक व्यक्ति न केवल डिजिटल माध्यमों का उपयोगकर्ता है, बल्कि वह एक जिम्मेदार, नैतिक और जागरूक नागरिक भी माना जाता है। डिजिटल नागरिकता का अर्थ केवल इंटरनेट तक पहुँच प्राप्त करना नहीं

है, बल्कि उसका सुरक्षित, जिम्मेदार और नैतिक उपयोग करना भी है। इसमें यह अपेक्षा की जाती है कि व्यक्ति ऑनलाइन संचार में मर्यादित भाषा का प्रयोग करे, दूसरों की निजता का सम्मान करे, और फेक न्यूज़ या गलत सूचना के प्रसार से बचे। इस प्रकार, डिजिटल समाज में नागरिकता केवल अधिकारों तक सीमित नहीं, बल्कि कर्तव्यों से भी जुड़ी हुई है। तकनीकी विकास के साथ समाज को अनेक सामाजिक लाभ (Social Benefits) प्राप्त हुए हैं। सबसे पहले, सूचना और सेवाओं की पहुँच पहले से कहीं अधिक बढ़ी है — गाँवों और दूरदराज़ इलाकों में भी डिजिटल भुगतान, ई-लर्निंग और सरकारी योजनाओं का लाभ मिल रहा है। दूसरा, डिजिटल मंचों ने संवाद और सहभागिता को लोकतांत्रिक रूप दिया है, जिससे प्रत्येक व्यक्ति अपनी आवाज़ उठा सकता है। तीसरा, डिजिटल उद्यमिता और ऑनलाइन व्यवसायों ने युवाओं के लिए नए अवसर खोले हैं। सुहल्का और राजपूत (2025) के अनुसार, विश्वविद्यालय स्तर पर डिजिटल जुड़ाव (digital engagement) ने छात्रों के सामाजिक और शैक्षिक विकास में सकारात्मक भूमिका निभाई है।

संक्षेप में कहा जाए तो आधुनिक समाज की डिजिटल निर्भरता केवल तकनीकी सुविधा का प्रतीक नहीं है, बल्कि यह सामाजिक परिवर्तन और सशक्तिकरण का भी माध्यम है। हालांकि यह निर्भरता तभी सकारात्मक परिणाम दे सकती है जब इसके साथ साइबर सुरक्षा, डिजिटल साक्षरता और नैतिकता की भावना समान रूप से विकसित की जाए।

2. साहित्य का अध्ययन

कुछ ताज़ा भारतीय अध्ययन इस बात को और पुष्ट करते हैं कि साइबर सुरक्षा केवल तकनीकी समस्या नहीं, बल्कि एक सामाजिक और शैक्षिक चुनौती भी है—

सुहल्का, जे., & राजपूत, पी. एस. (2025) के अध्ययन "Digital Engagement and Cyber Literacy among University Students in Southern Rajasthan" में यह पाया गया कि विश्वविद्यालय छात्रों में सोशल नेटवर्किंग साइटों का उपयोग अत्यधिक है, किंतु साइबर सुरक्षा प्रथाओं की जानकारी सीमित है। लगभग 84% छात्रों ने विश्वविद्यालय पाठ्यक्रम में साइबर सुरक्षा शिक्षा शामिल करने की आवश्यकता जताई।

पंजानी, एच., & मुड्गल, ए. (2025) ने अपने अध्ययन "A Study of Cyber Safety Awareness among Students and Educational Initiatives" में यह पाया कि 12–18 वर्ष के विद्यार्थियों में साइबर सुरक्षा

के प्रति जागरूकता में उल्लेखनीय अंतर है—मध्यम कक्षाओं के छात्र अपेक्षाकृत अधिक असुरक्षित पाए गए।

बारभुइया, आर. के. (2024) ने "Cyber-Safety: Concepts, Threats, and Essential Measures" शीर्षक से प्रकाशित अपने लेख में सुझाव दिया कि स्कूल और शिक्षक प्रशिक्षण पाठ्यक्रम में साइबर सुरक्षा और डिजिटल नैतिकता को शामिल किया जाना चाहिए, ताकि प्रारंभिक स्तर से ही सुरक्षा की संस्कृति विकसित हो सके।

चावला, वी., कपूर, वाई., & चावला, टी. (2023) के "Cybersecurity Awareness Amongst Youth — A Survey in Delhi/NCR" अध्ययन से यह स्पष्ट हुआ कि युवाओं में डिजिटल नैतिकता और सुरक्षित व्यवहार के प्रति ज्ञान सीमित है, और शिक्षण संस्थान इस दिशा में अभी पर्याप्त प्रयास नहीं कर रहे।

मनराल, एम. एस. (2025) द्वारा प्रकाशित NCRB Report for 2023 में यह बताया गया कि भारत में साइबर अपराधों में 31.2% की वृद्धि हुई है, जिनमें से अधिकांश मामले वित्तीय धोखाधड़ी और पहचान चोरी से जुड़े थे। यह आँकड़ा बताता है कि साइबर सुरक्षा अब राष्ट्रीय सुरक्षा और सामाजिक स्थिरता दोनों से जुड़ा हुआ मुद्दा है।

3. शोध कार्यप्रणाली (Research Methodology)

प्रस्तुत शोध पत्र का स्वरूप वर्णात्मक (Descriptive) एवं विश्लेषणात्मक (Analytical) है । इस अध्ययन में प्राथमिक रूप से द्वितीयक आँकड़ों (Secondary Data) का उपयोग किया गया है, जिन्हें विभिन्न सरकारी रिपोर्टों, प्रतिष्ठित शोध पत्रिकाओं और समाचार पत्रों से संकलित किया गया है ।

- **आँकड़ों का स्रोत:** शोध हेतु नेशनल क्राइम रिकॉर्ड्स ब्यूरो (NCRB) की वर्ष 2023 की रिपोर्ट, भारतीय दूरसंचार विनियामक प्राधिकरण (TRAI) की 2024 की सांख्यिकी और CERT-In की वार्षिक रिपोर्टों का विश्लेषण किया गया है ।
- **क्षेत्रीय संदर्भ:** अध्ययन की गहराई हेतु राजस्थान और दिल्ली/NCR क्षेत्र में विश्वविद्यालयी छात्रों पर किए गए हालिया सर्वेक्षणों (2023-2025) को आधार बनाया गया है ।

- **विश्लेषण का आधार:** शोध में तकनीकी पहलुओं के बजाय साइबर सुरक्षा के सामाजिक-मनोवैज्ञानिक (Socio-Psychological) और शैक्षिक (Educational) प्रभावों पर विशेष ध्यान केंद्रित किया गया है ।

4. विश्लेषण एवं परिणाम

भारत के संदर्भ में साइबर सुरक्षा केवल तकनीकी या प्रशासनिक नीति का मुद्दा नहीं है, बल्कि यह एक सामाजिक, शैक्षिक और नैतिक विषय भी बन गया है। देश के तीव्र डिजिटलीकरण—चाहे वह ई-गवर्नेंस हो, ऑनलाइन बैंकिंग, शिक्षा या स्वास्थ्य सेवाएँ—ने साइबर सुरक्षा की आवश्यकता को और भी महत्वपूर्ण बना दिया है। आज भारत विश्व का तीसरा सबसे बड़ा इंटरनेट उपयोगकर्ता देश है, और डिजिटल सेवाओं का विस्तार ग्रामीण क्षेत्रों तक हो चुका है (ट्राई रिपोर्ट, 2024)। लेकिन इस डिजिटल विस्तार के साथ ही साइबर अपराधों, डेटा चोरी और ऑनलाइन ठगी जैसी समस्याएँ भी तेजी से बढ़ रही हैं। भारत सरकार ने इस चुनौती का सामना करने के लिए कई योजनाएँ और संस्थागत ढाँचे तैयार किए हैं। राष्ट्रीय साइबर सुरक्षा नीति (National Cyber Security Policy, 2013) का उद्देश्य "सुरक्षित और लचीला साइबर स्पेस" स्थापित करना था। यह नीति सुरक्षा जागरूकता, क्षमता निर्माण, और डेटा संरक्षण जैसे मुद्दों पर केंद्रित थी। इसके अतिरिक्त, डिजिटल इंडिया मिशन (2015) ने न केवल नागरिकों को ऑनलाइन सेवाओं से जोड़ा, बल्कि ई-गवर्नेंस और पारदर्शिता को भी सुदृढ़ किया। वहीं CERT-In (Computer Emergency Response Team – India) भारत में साइबर घटनाओं की निगरानी और प्रतिक्रिया में प्रमुख भूमिका निभा रहा है। CERT-In की 2023 की वार्षिक रिपोर्ट के अनुसार, देश में लगभग 10 लाख से अधिक साइबर घटनाएँ दर्ज की गईं, जिनमें वित्तीय धोखाधड़ी, फ़िशिंग, और डेटा लीक के मामले सबसे प्रमुख थे (CERT-In, 2023)। फिर भी, भारत के शैक्षणिक संस्थानों में साइबर सुरक्षा के प्रति जागरूकता अब भी सीमित है। कई विश्वविद्यालयों और स्कूलों में डिजिटल साक्षरता तो पढ़ाई जाती है, परंतु साइबर नैतिकता (Cyber Ethics) और सुरक्षित व्यवहार के प्रशिक्षण की कमी है। सामाजिक और शैक्षिक दृष्टि से यह एक गंभीर चुनौती है, क्योंकि युवा वर्ग सबसे अधिक ऑनलाइन सक्रिय और साथ ही सबसे अधिक संवेदनशील भी है। सामाजिक संगठनों, मीडिया और गैर-सरकारी संस्थाओं ने इस दिशा में महत्वपूर्ण प्रयास किए हैं। इंटरनेट सेफ्टी वीक, साइबर जागरूकता अभियान, और विभिन्न मीडिया अभियानों ने आम नागरिकों को सतर्क किया है। फिर भी, डिजिटल नागरिकता का विचार तब तक सार्थक नहीं हो सकता जब तक नागरिक समाज में साइबर

नैतिकता की भावना विकसित न हो। यह नैतिकता केवल पासवर्ड या एन्क्रिप्शन तक सीमित नहीं, बल्कि ऑनलाइन आचरण, निजता का सम्मान और डिजिटल जिम्मेदारी की संस्कृति से जुड़ी है।

तालिका 1: भारत में साइबर अपराध का सांख्यिकीय विश्लेषण (2023-2025)

मानक (Parameter)	**विवरण / आँकड़े**	**स्रोत**
वार्षिक अपराध वृद्धि (2023)	31.2% की तीव्र वृद्धि	NCRB रिपोर्ट (मनराल, 2025)
पंजीकृत साइबर घटनाएँ	10 लाख से अधिक मामले (2023)	CERT-In वार्षिक रिपोर्ट
प्रमुख अपराध श्रेणी	वित्तीय धोखाधड़ी (Financial Fraud)	NCRB/CERT-In
इंटरनेट उपयोगकर्ता आधार	विश्व में तीसरा सबसे बड़ा (2024)	ट्राई (TRAI) रिपोर्ट, 2024

तालिका 1 के आँकड़ों का विश्लेषण करने पर यह स्पष्ट होता है कि भारत में डिजिटल क्रांति के साथ-साथ अपराधों के स्वरूप में भी 'पैराडाइम शिफ्ट' (Paradigm Shift) आया है। नेशनल क्राइम रिकॉर्ड्स ब्यूरो (NCRB) की 2023 की रिपोर्ट के अनुसार, साइबर अपराधों में 31.2% की वार्षिक वृद्धि यह दर्शाती है कि सुरक्षा उपाय तकनीकी विस्तार की गति के साथ तालमेल नहीं बिठा पा रहे हैं । अधिकांश मामलों का 'वित्तीय धोखाधड़ी' से जुड़ा होना यह बताता है कि अपराधी अब सीधे तौर पर डिजिटल अर्थव्यवस्था की नींव (बैंकिंग और UPI) पर प्रहार कर रहे हैं । 10 लाख से अधिक साइबर घटनाओं का दर्ज होना यह संकेत देता है कि साइबर सुरक्षा अब केवल एक तकनीकी विषय नहीं, बल्कि एक गंभीर राष्ट्रीय और सामाजिक चिंता बन चुकी है ।

तालिका 2: विश्वविद्यालय छात्रों में साइबर साक्षरता एवं व्यवहार (क्षेत्रीय अध्ययन)

अध्ययन का क्षेत्र (Location)	**मुख्य निष्कर्ष (Key Findings)**	**सुरक्षा जागरूकता स्थिति**
दक्षिण राजस्थान (2025)	84% छात्र पाठ्यक्रम में साइबर शिक्षा चाहते हैं	डिजिटल जुड़ाव उच्च, पर व्यावहारिक ज्ञान सीमित

दिल्ली/NCR (2023)	युवाओं में डिजिटल नैतिकता का अभाव	शिक्षण संस्थानों के प्रयास अपर्याप्त
स्कूली छात्र (12–18 वर्ष)	मध्यम कक्षाओं के छात्र अधिक असुरक्षित	जागरूकता के स्तर में उल्लेखनीय अंतर

तालिका 2 में प्रस्तुत क्षेत्रीय सर्वेक्षणों के परिणाम भारत के 'शिक्षण संस्थानों' की वर्तमान स्थिति पर गंभीर प्रश्न खड़े करते हैं:

- ज्ञान का अभाव: दक्षिण राजस्थान के विश्वविद्यालयी छात्रों का अध्ययन यह उजागर करता है कि केवल 'सोशल मीडिया' का उपयोग करना 'डिजिटल साक्षरता' नहीं है । छात्रों के पास तकनीकी पहुँच तो है, लेकिन व्यावहारिक सुरक्षा ज्ञान सीमित है।
- पाठ्यक्रम की माँग: 84% छात्रों द्वारा साइबर शिक्षा को अनिवार्य बनाने की माँग यह स्पष्ट करती है कि वर्तमान युवा पीढ़ी इस खतरे को पहचान रही है और औपचारिक मार्गदर्शन चाहती है ।
- संवेदनशीलता: दिल्ली/NCR और स्कूली छात्रों (12-18 वर्ष) के डेटा से यह सिद्ध होता है कि शिक्षण संस्थानों में साइबर नैतिकता और सुरक्षित ऑनलाइन व्यवहार के प्रशिक्षण की भारी कमी है, जिससे किशोर वर्ग साइबर बुलिंग और अन्य खतरों के प्रति अधिक संवेदनशील (vulnerable) हो गया है ।

अतः, यह शोध पत्र सिफारिश करता है कि उच्च शिक्षण संस्थानों को 'साइबर सुरक्षा' को केवल एक वैकल्पिक विषय न मानकर इसे 'क्रेडिट-बेस्ड' (Credit-based) अनिवार्य पाठ्यक्रम के रूप में अपनाना चाहिए।

तालिका 3: साइबर सुरक्षा: सामाजिक अवसर बनाम चुनौतियाँ

क्षेत्र (Sector)	**प्रमुख अवसर (Opportunities)**	**प्रमुख चुनौतियाँ (Challenges)**
आर्थिक (Economic)	डिजिटल अर्थव्यवस्था और फिनटेक नवाचार	यूपीआई/वॉलेट ठगी और बैंकिंग हैक्स
सामाजिक (Social)	डिजिटल नागरिकता और लोकतांत्रिक संवाद	साइबर बुलिंग और सामाजिक अलगाव
मनोवैज्ञानिक (Psychological)	ऑनलाइन समुदायों के माध्यम से अभिव्यक्ति	डिजिटल थकान और पहचान का संकट

शैक्षिक (Educational)	ई-लर्निंग और सूचना की समान पहुँच	डिजिटल अंतराल और सुरक्षा साक्षरता की कमी

तालिका 3 का तुलनात्मक विश्लेषण एक 'डिजिटल एम्बिवैलेंस' (Digital Ambivalence) की स्थिति को दर्शाता है:

- सशक्तिकरण बनाम असुरक्षा: जहाँ एक ओर डिजिटल इंडिया और ई-गवर्नेंस ने पारदर्शिता लाकर नागरिकों को सशक्त बनाया है, वहीं दूसरी ओर 'डेटा दुरुपयोग' और 'निजता का संकट' इस सशक्तिकरण को बाधित कर रहा है ।
- सामाजिक प्रभाव: ऑनलाइन समुदायों ने संवाद के नए अवसर दिए हैं, लेकिन साथ ही 'साइबर बुलिंग' और 'सामाजिक अलगाव' जैसी समस्याओं ने मानवीय संबंधों और मानसिक स्वास्थ्य पर नकारात्मक प्रभाव डाला है ।
- निष्कर्ष: यह स्पष्ट है कि डिजिटल समाज में 'अवसर' तभी स्थायी हो सकते हैं जब हम 'चुनौतियों' का समाधान नीतिगत, कानूनी और व्यक्तिगत—तीनों स्तरों पर करें ।

5. चर्चा

5.1. अवसर — साइबर सुरक्षा से समाज को होने वाले लाभ

आधुनिक समाज में साइबर सुरक्षा (Cyber Security) केवल खतरों से बचाव का माध्यम नहीं है, बल्कि यह अनेक सामाजिक और आर्थिक अवसरों (Socio-Economic Opportunities) का द्वार भी खोलती है। जैसे-जैसे डिजिटल सेवाओं का प्रसार बढ़ रहा है, वैसे-वैसे सुरक्षित साइबर ढाँचे की माँग भी बढ़ रही है, जो न केवल तकनीकी क्षेत्र में नवाचार को प्रोत्साहित करती है, बल्कि समाज में विश्वास, पारदर्शिता और समावेशन को भी मजबूत बनाती है।

सबसे पहले, डिजिटल अर्थव्यवस्था का विस्तार (Expansion of Digital Economy) साइबर सुरक्षा पर निर्भर है। भारत की अर्थव्यवस्था तेजी से डिजिटल मोड में रूपांतरित हो रही है — डिजिटल पेमेंट, ई-कॉमर्स, ऑनलाइन बैंकिंग, और फिनटेक स्टार्टअप्स के माध्यम से लेन-देन की प्रकृति बदल चुकी है। यदि सुरक्षा प्रणाली सुदृढ़ हो, तो उपभोक्ता का भरोसा बढ़ता है, जिससे डिजिटल लेन-देन और भी तीव्र गति से बढ़ते हैं। त्रिपाठी (2025) के अनुसार, भारत में पिछले दशक में साइबर सुरक्षा ढांचे के विस्तार ने डिजिटल व्यापार और वित्तीय नवाचार के लिए सुरक्षित वातावरण तैयार किया है। दूसरा,

साइबर सुरक्षा ने रोजगार और नवाचार (Employment and Innovation) के नए क्षेत्र उत्पन्न किए हैं। अब साइबर विश्लेषक, डेटा प्रोटेक्शन अधिकारी, एथिकल हैकर, और साइबर फोरेंसिक विशेषज्ञ जैसी नौकरियाँ तेजी से बढ़ रही हैं। इससे युवाओं के लिए तकनीकी और अनुसंधान आधारित रोजगार के अवसर पैदा हो रहे हैं। बारभुइया (2024) का मत है कि सुरक्षा तकनीकों में नवाचार जैसे एन्क्रिप्शन (Encryption), मल्टी-फैक्टर ऑथेंटिकेशन (Authentication) और बायोमेट्रिक सिस्टम्स न केवल तकनीकी रूप से सशक्त बनाते हैं, बल्कि सामाजिक विश्वास और आर्थिक स्थिरता को भी सुनिश्चित करते हैं। तीसरा, सरकारी नीतियों और सेवाओं में साइबर सुरक्षा के एकीकरण से पारदर्शिता और दक्षता (Transparency and Efficiency) बढ़ी है। उदाहरण के लिए, आधार-आधारित सत्यापन और डिजिटल लॉकर जैसी सेवाओं ने दस्तावेज़ी धोखाधड़ी को कम किया है तथा ई-गवर्नेंस को विश्वसनीय बनाया है। पंजानी एवं मुड्गल (2025) ने अपने अध्ययन में पाया कि शिक्षण संस्थानों में साइबर सुरक्षा कार्यक्रमों के चलते छात्रों में न केवल सुरक्षा जागरूकता बढ़ी है, बल्कि वे सरकारी डिजिटल सेवाओं का अधिक भरोसे के साथ उपयोग करने लगे हैं। चौथा, साइबर सुरक्षा सामाजिक दृष्टि से समावेशन और समान सूचना पहुंच (Social Inclusion and Equal Access to Information) को भी सशक्त बनाती है। जब लोग डिजिटल प्लेटफॉर्मों पर सुरक्षित महसूस करते हैं, तो महिलाएँ, ग्रामीण समुदाय, वरिष्ठ नागरिक और सामाजिक रूप से वंचित वर्ग भी इन सेवाओं से लाभान्वित होते हैं। इस प्रकार, साइबर सुरक्षा डिजिटल लोकतंत्र और समान अवसरों के विकास में योगदान देती है।

अंततः, सुरक्षा तकनीकों के विकास के साथ-साथ जागरूकता कार्यक्रम (Awareness Programs) और डिजिटल साक्षरता ने सामाजिक भरोसे (Social Trust) को मजबूत किया है। **सुहल्का और राजपूत (2025)** ने पाया कि साइबर साक्षरता और सुरक्षित ऑनलाइन व्यवहार का सीधा संबंध डिजिटल प्लेटफॉर्मों के उपयोग में आत्मविश्वास से है। जब समाज साइबर सुरक्षा को अपनी साझा जिम्मेदारी मानता है, तब डिजिटल विकास टिकाऊ और न्यायसंगत बनता है।

5.2. चुनौतियाँ — सामाजिक दृष्टि से प्रमुख समस्याएँ और उनके प्रभाव

जहाँ अवसर हैं, वहां चुनौतियाँ भी समान रूप से गंभीर हैं। सामाजिक विज्ञान के दृष्टिकोण से ये चुनौतियाँ अक्सर तकनीकी नहीं बल्कि **व्यवहारिक, सांस्कृतिक और नीतिगत** होती हैं। नीचे प्रमुख चुनौतियों का विस्तार दिया गया है:

5.2.1. साइबर अपराध और आर्थिक ठगी : वित्तीय ऑनलाइन धोखाधड़ी, मोबाइल वॉलेट/UPI पर ठगी, फिशिंग और बैंकिंग हैक्स बड़े पैमाने पर बढ़े हैं। राष्ट्रीय स्तर पर दर्ज हुए मामलों की संख्या में हालिया वर्षों में तीव्र वृद्धि देखी गयी है—जो बताती है कि डिजिटल पहुँच बढ़ने के साथ धोखाधड़ी और उसका सामाजिक प्रभाव (नुकसान, विश्वास की कमी) भी बढ़ा है। यह न केवल आर्थिक हानि का कारण बनता है बल्कि सार्वजनिक व्यवस्था और सामाजिक भरोसे को भी प्रभावित करता है। (दी इंडियन एक्सप्रेस 2025)

5.2.2. निजता और डेटा दुरुपयोग (Privacy and Data Misuse) : डिजिटल लेन-देन और सोशल मीडिया उपयोग से व्यक्तिगत डेटा का विशाल भण्डार बनता है। इसके परिणामस्वरूप निजता का संकट, प्रोफ़ाइलिंग, लक्ष्य-निर्मित विज्ञापन और संवेदनशील जानकारियों का दुरुपयोग संभावित होता है। सामाजिक दृष्टि से यह समस्या असमान शक्ति-संबंध (power asymmetries) उत्पन्न कर सकती है—जहाँ बड़े संगठन और प्लेटफॉर्म व्यक्तिगत डेटा के माध्यम से निर्णय-शक्ति जमा कर लेते हैं।

5.2.3. मनोवैज्ञानिक प्रभाव और साइबर बुलिंग : सोशल मीडिया और डिजिटल संचार ने समाज में बातचीत के स्वर बदल दिए हैं—पर इनका दुष्प्रभाव विशेषकर किशोरों और युवाओं पर स्पष्ट दिखता है। साइबर बुलिंग, ऑनलाइन गलतफहमियाँ, पहचान-आधारित उत्पीड़न और मानसिक तनाव से सम्बन्धित अध्ययन बताते हैं कि भारत में भी युवा वर्ग पर इन घटनाओं का गंभीर असर है। कई अनुसंधान और समिक्षाएँ इस बात की ओर इंगित करती हैं कि साइबर बुलिंग के परिणाम—डिप्रेशन, एंग्ज़ाइटी और आत्महत्या-प्रवृत्तियाँ—गंभीर सामाजिक चुनौतियाँ उत्पन्न कर सकती हैं। (विजयरानी, 2024)

5.2.4. फेक न्यूज़ और सूचना-प्रसार का विकृत प्रभाव : सोशल मीडिया पर गलत जानकारी तेजी से फैलती है—यह विकृत सूचना लोकतांत्रिक प्रक्रियाओं, सार्वजनिक स्वास्थ्य संदेशों और सामुदायिक सहवास को प्रभावित कर सकती है। समाजशास्त्रीय दृष्टि से यह भरोसे और सामूहिक निर्णय की गुणवत्ता में गिरावट का कारण बनता है।

5.2.5. डिजिटल असमानता और साक्षरता की कमी : डिजिटल साक्षरता (digital literacy) का अंतर—शहरी और ग्रामीण, आय-आधारित या शैक्षिक आधार पर—सामाजिक असमानताओं को और बढ़ा सकता है। जहां कुछ नागरिक नई सुविधाओं का लाभ उठाते हैं, वहीं अन्य सुविधाओं और सुरक्षा ज्ञान से वंचित रहकर और अधिक जोखिम में पड़ जाते हैं। कई शैक्षणिक सर्वे बताते हैं कि विश्वविद्यालय

और स्वास्थ्य संस्थान में भी साइबर सुरक्षा जागरूकता पर्याप्त नहीं है—जिसका नकारात्मक प्रभाव संस्थागत डेटा और सेवा-विश्वास पर पड़ता है। (कुम्भकर, 2025)

5.2.6. कानूनी और संस्थागत चुनौतियाँ : कई बार साइबर अपराध सीमाओं-आधारित (transnational) होते हैं—जिससे जाँच, सबूत-प्रवर्तन और न्यायिक प्रक्रियाएँ जटिल बन जाती हैं। भारत ने कई नीतिगत पहलें की हैं परंतु कानूनों का कार्यान्वयन, मानव-संसाधन और तकनीकी क्षमता में अंतर अभी भी एक चुनौती है। CERT-In, NCCC और अन्य संस्थाएँ सक्रिय हैं, पर बढ़ते हमलों व जटिलताओं का सामना करने के लिए सतत सुधार आवश्यक है।

5.3. समाजशास्त्रीय और मनोवैज्ञानिक परिप्रेक्ष्य — पहचान, भरोसा और नैतिकता

साइबर सुरक्षा का प्रश्न केवल तकनीकी नहीं, बल्कि गहराई से समाजशास्त्रीय और मनोवैज्ञानिक भी है। डिजिटल युग में व्यक्ति की पहचान, सामाजिक संबंध, और विश्वास की संरचना नए रूप में सामने आ रही है। यह वह दौर है जहाँ व्यक्ति का साइबर व्यवहार (Cyber Behaviour) उसकी सामाजिक छवि और मनोवैज्ञानिक स्थिति दोनों को प्रभावित करता है। सोशल मीडिया, ऑनलाइन समुदायों और डिजिटल प्लेटफॉर्मों ने मनुष्य को अपनी राय और व्यक्तित्व व्यक्त करने की नई स्वतंत्रता दी है, किंतु साथ ही उन्होंने पहचान की नई समस्याएँ भी उत्पन्न की हैं। आज एक व्यक्ति की ऑनलाइन पहचान (Online Identity) कई रूपों में विभाजित है—व्यक्तिगत, पेशेवर और सामाजिक। इस डिजिटल बहु-परिचय (multiple identity) की स्थिति में व्यक्ति कई बार आभासी छवि को वास्तविकता से अधिक महत्व देने लगता है। चावला, कपूर एवं चावला (2023) के अनुसार, युवाओं में ऑनलाइन स्वीकृति (social validation) की चाह इतनी प्रबल हो रही है कि वे व्यक्तिगत गोपनीयता और सुरक्षा के पहलुओं को अनदेखा कर देते हैं। यही प्रवृत्ति साइबर बुलिंग, ट्रोलिंग और डिजिटल थकान जैसी मानसिक समस्याओं का कारण बन रही है। दूसरी ओर, तकनीकी प्रगति और डिजिटल निर्भरता ने समाज में सामाजिक अलगाव (Social Isolation) की नई स्थितियाँ उत्पन्न की हैं। व्यक्ति आभासी संवाद में तो सक्रिय है, परंतु वास्तविक सामाजिक संबंधों में दूरी बढ़ रही है। परिवार और समुदाय के साथ पारस्परिक संवाद सीमित होता जा रहा है। पंजानी एवं मुड्गल (2025) के अध्ययन में यह पाया गया कि छात्रों का स्क्रीन टाइम बढ़ने से सामाजिक संवाद और सहानुभूति में कमी देखी गई। यह स्थिति "टेक्नोलॉजिकल कनेक्टिविटी" के बावजूद "इमोशनल डिसकनेक्शन" की ओर संकेत करती है। यहां एक महत्वपूर्ण द्वंद्व उभरता है — "स्मार्ट सोसाइटी" बनाम "सुरक्षित सोसाइटी" का। तकनीकी दृष्टि से

जितना अधिक समाज स्मार्ट बनता जा रहा है, उतनी ही उसकी सुरक्षा चिंताएँ भी गहरी हो रही हैं। स्मार्ट शहरों, एआई-आधारित निगरानी प्रणालियों और इंटरनेट ऑफ थिंग्स (IoT) जैसे नवाचारों ने जीवन को सुविधाजनक बनाया है, लेकिन साथ ही निजता और डाटा सुरक्षा पर खतरे भी बढ़ाए हैं। त्रिपाठी (2025) का मत है कि बिना नैतिक दिशा-निर्देशों के तकनीकी नवाचार "डिजिटल असुरक्षा" का नया रूप ले सकते हैं। इसलिए "स्मार्टनेस" का अर्थ केवल तकनीकी दक्षता नहीं, बल्कि सुरक्षा और मानव गरिमा की रक्षा भी होना चाहिए।

अंततः, डिजिटल संस्कृति में विश्वास (Trust) और भय (Fear) का एक साथ सह-अस्तित्व दिखाई देता है। एक ओर लोग डिजिटल प्लेटफार्मों के माध्यम से अवसरों, सेवाओं और संवादों का आनंद ले रहे हैं, वहीं दूसरी ओर उन्हें डेटा चोरी, ऑनलाइन ठगी या गलत सूचना का भय सताता है। यह द्वंद्व समाज में "डिजिटल एम्बिवैलेंस" (digital ambivalence) की स्थिति उत्पन्न करता है — जहाँ विकास और असुरक्षा एक साथ चलते हैं। इस मनोवैज्ञानिक असंतुलन को दूर करने के लिए साइबर नैतिकता, डिजिटल साक्षरता और भावनात्मक संतुलन की शिक्षा को बढ़ावा देना आवश्यक है।

6. समाधान और व्यवहारिक सुझाव — सामाजिक विज्ञान के दृष्टिकोण से नीतियाँ और अभ्यास

साइबर सुरक्षा केवल तकनीकी उपायों तक सीमित नहीं है; यह समाज, शिक्षा और नीति निर्माण का सम्मिलित प्रयास मांगती है। भारत जैसे डिजिटल रूप से तेजी से उभरते देश में इस दिशा में ठोस कदम उठाना अत्यंत आवश्यक है। सबसे पहले, साइबर साक्षरता (Cyber Literacy) और जागरूकता अभियान समाज के प्रत्येक वर्ग तक डिजिटल सुरक्षा की जानकारी पहुँचाने में निर्णायक भूमिका निभाते हैं। सरकारी और गैर-सरकारी संस्थाओं द्वारा आयोजित ऑनलाइन सुरक्षा कार्यशालाएँ, डिजिटल जागरूकता सप्ताह, और मीडिया अभियानों ने लोगों में साइबर खतरे के प्रति सतर्कता बढ़ाई है। बारभुइया (2024) के अनुसार, प्रारंभिक शिक्षा में साइबर सुरक्षा विषय को शामिल करने से छात्रों में ऑनलाइन सुरक्षित व्यवहार और जिम्मेदारी की भावना विकसित होती है।

दूसरा, विद्यालय और विश्वविद्यालय स्तर पर साइबर शिक्षा का समावेश अनिवार्य होना चाहिए। इसके तहत पासवर्ड सुरक्षा, डेटा संरक्षण, फिशिंग और साइबर अपराध की पहचान जैसी प्रथाओं को पढ़ाया जा सकता है। सुहल्का और राजपूत (2025) के अध्ययन में यह पाया गया कि विश्वविद्यालय छात्रों में डिजिटल जुड़ाव तो अधिक था, लेकिन साइबर सुरक्षा के व्यावहारिक ज्ञान की कमी थी। लगभग 84%

छात्रों ने इस विषय को पाठ्यक्रम में शामिल करने का समर्थन किया। इसके अतिरिक्त, पंजानी एवं मुद्गल (2025) ने स्कूल स्तर पर अध्ययन करते हुए पाया कि 12–18 वर्ष के छात्रों में साइबर जागरूकता काफी असमान है, और इसे बढ़ाने के लिए विद्यालयों में नियमित प्रशिक्षण कार्यक्रम आवश्यक हैं। तीसरा, कड़े साइबर कानून और उनका प्रभावी क्रियान्वयन आवश्यक हैं। भारत में Information Technology Act, 2000 और CERT-In जैसी संस्थाएँ साइबर अपराधों के खिलाफ सक्रिय हैं, किंतु कानूनों की गति, संसाधनों की कमी और मामलों की लंबी प्रक्रिया सुरक्षा के प्रभाव को सीमित कर देती है। मनराल (2025) की रिपोर्ट के अनुसार, साइबर अपराधों में लगातार वृद्धि हो रही है, और इस स्थिति में कानून का त्वरित कार्यान्वयन और व्यापक जागरूकता दोनों आवश्यक हैं। चौथा, व्यक्तिगत स्तर पर सावधानी और डिजिटल अनुशासन अपनाना भी अत्यंत महत्वपूर्ण है। इसमें मजबूत पासवर्ड का उपयोग, दो-स्तरीय प्रमाणीकरण, संदिग्ध लिंक से बचाव, और सोशल मीडिया पर व्यक्तिगत जानकारी साझा करते समय सतर्कता शामिल है। चावला, कपूर एवं चावला (2023) के अध्ययन से यह स्पष्ट हुआ कि युवाओं में सुरक्षा प्रथाओं का पालन सीमित है, जिससे साइबर जोखिम बढ़ता है।

अंततः, सामाजिक-तकनीकी सहयोग (Public–Private Partnership) का मॉडल अपनाना चाहिए। इसमें सरकारी संस्थान, निजी टेक्नोलॉजी कंपनियाँ, शिक्षा संस्थान और नागरिक संगठन मिलकर साइबर सुरक्षा के नवाचार, जागरूकता अभियान और रिसर्च प्रोग्राम चला सकते हैं। इस तरह का सहयोग न केवल तकनीकी समाधान उपलब्ध कराता है, बल्कि समाज में सुरक्षा-संवेदनशीलता और भरोसे की भावना भी विकसित करता है। इस प्रकार, एक समग्र दृष्टिकोण जिसमें शिक्षा, नीति, व्यक्तिगत अनुशासन और सार्वजनिक-निजी साझेदारी शामिल हो, वह भारतीय समाज में सुरक्षित और सशक्त डिजिटल वातावरण के निर्माण की दिशा में निर्णायक साबित हो सकता है।

7. निष्कर्ष — सुरक्षित डिजिटल समाज की ओर

आधुनिक समाज में साइबर सुरक्षा सिर्फतकनीकी उपकरणों या विशेषज्ञों की जिम्मेदारी नहीं है। यह नागरिकों, संस्थाओं, सरकारों और नीति निर्माताओं की सामूहिक जिम्मेदारी है। जब समाज में जागरूकता बढ़ेगी, शिक्षा मजबूत होगी, नीतियाँ पारदर्शी एवं न्यायसंगत होंगी, और ऑनलाइन व्यवहार की नैतिकता को महत्त्व मिलेगा — तभी डिजिटल लाभ सुरक्षित रूप से उपयोगी होंगे। भारत में हाल ही के आँकड़े यह बताते हैं कि साइबर अपराधों की संख्या में बहुत वृद्धि हुई है, और उनमें से

अधिकांश धोखाधड़ी संबंधित हैं (मनराल, 2025)। साथ ही, अनेक अध्ययन यह दर्शाते हैं कि शिक्षा संस्थानों में साइबर सुरक्षा जागरूकता अभी भी पर्याप्त नहीं है (सुहल्का और राजपूत, 2025; चावला, कपूर एवं चावला, 2023)। यह समय है कि सामाजिक विज्ञान के अध्ययन, शिक्षा नीति, सार्वजनिक जागरूकता अभियान और कानूनी तंत्र मिलकर एक सुरक्षित, समावेशी और विश्वसनीय डिजिटल समाज की नींव रखें।

सन्दर्भ सूची

कर्ट-इन (CERT-In). (2023). *वार्षिक रिपोर्ट 2023*. इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार.

कुम्भकर, एस. (2025). शैक्षणिक संस्थानों में डेटा सुरक्षा और निजता के प्रति संवेदनशीलता. *जर्नल ऑफ डेटा एथिक्स*, 4(1), 112-125.

चावला, वी., कपूर, वाई., एवं चावला, टी. (2023). दिल्ली/एनसीआर में युवाओं में साइबर सुरक्षा जागरूकता — एक सर्वेक्षण. *इंडियन जर्नल ऑफ कंप्यूटर साइंस*, 8(2), 42–52.

ट्राई (TRAI) रिपोर्ट. (2024). *भारत में टेलिकॉम और इंटरनेट उपयोग सांख्यिकी 2024*. टेलिकॉम रेगुलेटरी अथॉरिटी ऑफ इंडिया.

त्रिपाठी, एस. एस. (2025). भारत में पिछले दशक में साइबर अपराधों का व्यापक सर्वेक्षण. *आर्काइव प्रीप्रिंट arXiv:2505.23770*.

पंजानी, एच., एवं मुड्गल, ए. (2025). छात्रों में साइबर सुरक्षा जागरूकता और शैक्षणिक पहल पर अध्ययन. *इंडियन जर्नल ऑफ एजुकेशनल टेक्नोलॉजी*, 7(2), 246–256.

बारभुइया, आर. के. (2024). साइबर-सुरक्षा: अवधारणाएँ, खतरें और आवश्यक उपाय. *इंडियन जर्नल ऑफ साइबर स्टडीज*, 6(1), 15–28.

मनराल, एम. एस. (2025). *एनसीआरबी रिपोर्ट 2023: साइबर अपराधों में 31.2% की वृद्धि*. द इंडियन एक्सप्रेस.

इलेक्ट्रोनिकी एवं सूचना प्रौद्योगिकी मंत्रालय (MeitY). (2013). *राष्ट्रीय साइबर सुरक्षा नीति (National Cyber Security Policy) - 2013*. संचार और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार.

विजयरानी, आर. (2024). साइबर बुलिंग और युवाओं पर इसके मनोवैज्ञानिक प्रभाव: एक समाजशास्त्रीय अध्ययन. *इंडियन जर्नल ऑफ बिहेवियरल साइंसेज*, 12(3), 88-102.

सुहल्का, जे., एवं राजपूत, पी. एस. (2025). दक्षिण राजस्थान के विश्वविद्यालय छात्रों में डिजिटल जुड़ाव और साइबर साक्षरता. *जर्नल ऑफ सोशल इन्फॉर्मेटिक्स*, 9(1), 34–47.