ग्रामीण क्षेत्रों में साइबर सुरक्षा और डिजिटल नैतिकता

सतीश सिंह

ग्रामीण भारत तेज़ी से डिजिटल परिवर्तन के दौर से गुज़र रहा है, जहाँ इंटरनेट की पहुँच और स्मार्टफोन का उपयोग अभूतपूर्व गति से बढ़ रहा है। वर्ष 2026 तक, भारत के आधे से अधिक इंटरनेट उपयोगकर्ता ग्रामीण क्षेत्रों में निवास करते हैं जिसे किफायती डेटा, बेहतर कनेक्टिविटी और सरकारी पहलों का समर्थन प्राप्त है। ऑनलाइन बैंकिंग, यूपीआई, टेलीमेडिसिन और ई-लर्निंग जैसी डिजिटल सेवाएं अब अधिक सुलभ होती जा रही हैं, जिससे आजीविका और अवसरों तक पहुँच में बदलाव आ रहा है। हालाँकि, इस प्रगति के साथ नई चुनौतियाँ भी सामने आई हैं। सीमित वित्तीय साक्षरता और जागरूकता के कारण ग्रामीण उपयोगकर्ता साइबर धोखाधड़ी और ऑनलाइन जोखिमों के प्रति अधिक संवेदनशील हो गए हैं। इसलिए, सुरक्षित और समावेशी डिजिटल विकास सुनिश्चित करने के लिए साइबर सुरक्षा को मज़बूत करना और डिजिटल नैतिकता को बढ़ावा देना अत्यंत आवश्यक है।

तेज़ी से बढ़ती तकनीक के समय में ग्रामीण क्षेत्रों के सामने साइबर सुरक्षा और डिजिटल नैतिकता से जुड़े कई नए अवसर और चुनौतियाँ सामने आ रहे हैं। जैसे-जैसे गाँवों में इंटरनेट की पहुँच बढ़ रही है, वैसे-वैसे बैंकिंग जानकारी जैसे संवेदनशील डेटा की सुरक्षा अत्यंत महत्वपूर्ण हो गई है। 'साइबर सुरक्षा' का मतलब है- इंटरनेट, कंप्यूटर और डेटा को गलत लोगों की पहुँच से बचाना। लेकिन ग्रामीण क्षेत्रों में अक्सर इसके लिए पर्याप्त जानकारी, संसाधन और विशेषज्ञों की कमी होती है। इसी कारण गाँवों के लोग फ़िशिंग, ऑनलाइन ठगी और रैनसमवेयर जैसे साइबर हमलों का आसानी से शिकार बन सकते हैं। इसके साथ-साथ डिजिटल तकनीक के नैतिक पहलुओं पर भी ध्यान देना आवश्यक है। डिजिटल नैतिकता का संबंध डेटा की गोपनीयता, सुरक्षित इंटरनेट उपयोग और डिजिटल असमानता जैसे मुद्दों से है। यह ज़रूरी है कि ऐसे नियम और दिशानिर्देश हों जो लोगों की जानकारी को सुरक्षित रखें और सभी को डिजिटल संसाधनों तक समान पहुँच दें।

साइबर सुरक्षा को मज़बूत करने के साथ-साथ डिजिटल साक्षरता में सुधार करना भी बहुत महत्वपूर्ण है। गाँव के लोगों को यह सिखाना ज़रूरी है कि इंटरनेट का सुरक्षित उपयोग कैसे करें, मज़बूत पासवर्ड कैसे बनाएँ और अपनी व्यक्तिगत जानकारी को कैसे सुरक्षित रखें। अगर साइबर सुरक्षा और नैतिक मूल्यों को ध्यान में रखा जाए तो ग्रामीण समुदायों को साइबर खतरों से बेहतर तरीके से बचाया जा सकता है और एक सुरक्षित

लेखक वरिष्ठ बैंकिंग एवं आर्थिक स्तंभकार हैं और भारतीय स्टेट बैंक (मुंबई) के कॉर्पोरेट सेंटर में सहायक महाप्रबंधक हैं।
ईमेलः satish5249@gmail.com

तथा जागरूक डिजिटल समाज बनाया जा सकता है। इसके लिए ग्रामीण लोगों, व्यवसायों और प्रशासन के बीच सहयोग बहुत ज़रूरी है।

परिचय

भारत में जनवरी 2026 तक लगभग 95.8 करोड़ सक्रिय इंटरनेट उपयोगकर्ता थे, जिनमें से 54.8 करोड़ (57%) ग्रामीण क्षेत्रों से हैं। इंटरनेट का यह तेज़ विस्तार मुख्य रूप से स्मार्टफोन की बढ़ती पहुँच और सस्ती डेटा सेवाओं के कारण संभव हुआ है। अनुमान है कि वर्ष 2026 तक स्मार्टफोन उपयोगकर्ताओं की संख्या 100 करोड़ से अधिक हो जाएगी। ग्रामीण क्षेत्रों में स्मार्टफोन का उपयोग हर साल लगभग 6% की दर से बढ़ रहा है, जबकि शहरी क्षेत्रों में यह वृद्धि लगभग 2.5% है।

डिजिटल परिवर्तन को बढ़ावा देने के लिए देशभर में 4,09,111 से अधिक सार्वजनिक वाई-फाई हॉटस्पॉट स्थापित किए गए हैं। साथ ही 'भारतनेट परियोजना' के तहत 2,15,000 से अधिक ग्राम पंचायतों को तेज़ गति वाले इंटरनेट से जोड़ा गया है। मोबाइल सेवा प्रदाता अब 5G सेवाएँ भी उपलब्ध करा रहे हैं, जिससे टेलीमेडिसिन और ई-शिक्षा जैसी सुविधाओं तक पहुँच आसान हो रही है।

सरकार की योजनाओं में कृत्रिम बुद्धिमत्ता (AI) का उपयोग भी किया जा रहा है। उदाहरण के तौर पर, प्रधानमंत्री आवास योजना (ग्रामीण) में धोखाधड़ी रोकने के लिए एआई तकनीक का उपयोग किया जा रहा है। डिजिटल लेन-देन को बढ़ावा देने के लिए 1,49,000 से अधिक 'बैंक सखियों' को जोड़ा गया है और मनरेगा की 99% से अधिक मज़दूरी सीधे लाभ अंतरण (DBT) या इलेक्ट्रॉनिक माध्यम से दी जा रही है। हालाँकि इन प्रयासों के बावजूद ग्रामीण क्षेत्रों में वित्तीय और डिजिटल साक्षरता अभी भी कम है, जिसके कारण साइबर धोखाधड़ी के मामले बढ़ रहे हैं।

वित्तीय जागरूकता की कमी

डिजिटलीकरण ने ग्रामीण भारत में विकास के नए अवसर पैदा किए हैं और गाँव के लोगों के लिए वित्तीय सेवाओं का उपयोग आसान बनाया है। लेकिन इन क्षेत्रों में वित्तीय साक्षरता की कमी के कारण ऑनलाइन धोखाधड़ी का खतरा भी काफ़ी बढ़ गया है। डिजिटल खतरों को पहचानने और उनसे बचने के लिए वित्तीय जागरूकता बहुत ज़रूरी है, लेकिन इस मामले में ग्रामीण भारत अभी भी पीछे है।

राष्ट्रीय सांख्यिकी कार्यालय (NSO) की वर्ष 2023-24 की रिपोर्ट के अनुसार, ग्रामीण क्षेत्रों में सात वर्ष और उससे अधिक आयु की आबादी की साक्षरता दर 77.5% है, जो वर्ष 2011 में 67.77% थी। इस रिपोर्ट के अनुसार पुरुषों की साक्षरता दर 84.7% और महिलाओं की 70.4% है।

इसी तरह नाबार्ड वित्तीय समावेशन सर्वेक्षण वर्ष 2021-22 के अनुसार, ग्रामीण भारत में लगभग 51.3% लोग वित्तीय रूप से साक्षर हैं, जो वर्ष 2016-17 में 33.9% थी। हालाँकि इसमें सुधार हुआ है, फिर भी बड़ी संख्या में लोग अभी भी वित्तीय जानकारी से वंचित हैं।

वित्तीय जागरूकता की कमी के कारण ग्रामीण लोग अक्सर यह पहचान नहीं पाते कि पैसे गलती से किसी गलत खाते में चले गए हैं या फिर फर्ज़ी क्यूआर कोड, ऑनलाइन ठगी और अन्य डिजिटल धोखाधड़ी का शिकार हो रहे हैं। यूपीआई जैसे लोकप्रिय डिजिटल भुगतान माध्यमों का उपयोग करते समय भी कई बार लोग इन धोखाधड़ियों को समझ नहीं पाते और उन्हें आर्थिक नुकसान उठाना पड़ता है।

इसके अलावा, इंटरनेट बैंकिंग और मोबाइल बैंकिंग जैसे डिजिटल माध्यमों से लेन-देन करते समय भी जोखिम बढ़ जाता है, क्योंकि पर्याप्त जानकारी न होने के कारण लोग साइबर अपराधियों के जाल में फँस सकते हैं।

साइबर जोखिमों के प्रकार

वर्तमान समय में ऑनलाइन धोखाधड़ी कई माध्यमों से की जा रही है। इनमें सबसे अधिक मामले यूपीआई के माध्यम से सामने आते हैं, जहाँ ठग नकली यूपीआई आईडी बनाकर या फर्ज़ी QR कोड के जरिए लोगों को धोखा देते हैं। इसके अलावा, साइबर अपराधी बेटिंग ऐप्स का इस्तेमाल, नकली ऑनलाइन लोन ऐप जारी करना, फर्ज़ी सरकारी योजनाओं के नाम पर ठगी करना और सोशल मीडिया पर नकली प्रोफाइल बनाकर लोगों को गुमराह करना जैसे तरीकों का भी सहारा लेते हैं।

इसके अतिरिक्त, कई अन्य प्रकार की ठगी भी सामने आ रही हैं, जैसे आधार और पैन नंबर का दुरुपयोग, वन-टाइम पासवर्ड (OTP) चोरी करना, 'डिजिटल अरेस्ट' स्कैम, पार्सल और कूरियर से जुड़ी धोखाधड़ी, फर्ज़ी होटल बुकिंग तथा व्हाट्सऐप और टेलीग्राम जैसे मैसेजिंग ऐप्स पर इनाम या ऑफर से जुड़े लिंक भेजकर लोगों को फँसाना। साइबर अपराधी अक्सर संदिग्ध लिंक, फर्ज़ी SMS, फिशिंग संदेश, बैंक अधिकारी बनकर कॉल करना और KYC अपडेट के नाम पर ठगी जैसे तरीकों का भी इस्तेमाल करते हैं।

चौंकाने वाली बात यह है कि इन ऑनलाइन अपराधों का शिकार केवल आम लोग ही नहीं बल्कि पुलिस अधिकारी, न्यायाधीश, IAS अधिकारी, राजनेता, मंत्री और बैंक कर्मचारी जैसे शिक्षित लोग भी हो रहे हैं। इसी कारण, हाल के वर्षों में साइबर अपराधों के मामलों में तेज़ी से बढ़ोतरी हुई है और वर्ष 2021 से वर्ष 2024 के बीच इनकी संख्या लगभग 400% तक बढ़ गई है।

साइबर धोखाधड़ी से बढ़ता आर्थिक नुकसान

हाल के वर्षों में भारत में साइबर धोखाधड़ी के मामलों में तेज़ी से बढ़ोतरी हुई है। गृह मंत्रालय के हालिया आँकड़ों के अनुसार, वर्ष 2024 में लगभग 22,845 करोड़ रुपये की साइबर

ठगी हुई, जो वर्ष 2023 की तुलना में 200% से अधिक वृद्धि को दर्शाता है। यह प्रवृत्ति वर्ष 2025 में भी जारी रही, जहाँ साइबर धोखाधड़ी से होने वाला नुकसान लगभग 22,495 करोड़ रुपये तक पहुँच गया। इसमें बड़ी संख्या में मामलों का संबंध तथाकथित 'डिजिटल अरेस्ट' स्कैम से रहा है।

साइबर अपराधी लगातार नए-नए तरीके अपनाकर लोगों को ठग रहे हैं, जिससे बड़ी मात्रा में धन का नुकसान हो रहा है। इन अपराधियों की चालें इतनी जटिल होती हैं कि आम नागरिक के लिए उन्हें समझ पाना अक्सर मुश्किल हो जाता है। इसी कारण वर्ष 2021 से वर्ष 2025 के बीच कुल मिलाकर लगभग 52,976 करोड़ रुपये साइबर धोखाधड़ी में खो दिए गए। यह स्थिति स्पष्ट रूप से दिखाती है कि साइबर अपराध आज हमारे देश के सामने एक गंभीर चुनौती बनकर उभर रहा है।

साइबर धोखाधड़ी से बचने के उपाय

साइबर धोखाधड़ी से बचाव के लिए यह ज़रूरी है कि मोबाइल ऐप और सॉफ्टवेयर केवल विश्वसनीय और आधिकारिक स्रोतों से ही डाउनलोड किए जाएँ। समय-समय पर अपने मोबाइल या कंप्यूटर के ऑपरेटिंग सिस्टम और एंटीवायरस सॉफ्टवेयर को अपडेट करना भी आवश्यक है, ताकि नए साइबर खतरों से सुरक्षा बनी रहे। जब कंप्यूटर का उपयोग न किया जा रहा हो तो उसे लॉक रखना चाहिए और यह सुनिश्चित करना चाहिए कि फायरवॉल हमेशा सक्रिय रहे।

ऑनलाइन बैंकिंग करते समय एक अलग बैंक खाते का उपयोग करना भी सुरक्षित माना जाता है, जिसमें केवल आवश्यक राशि ही रखी जाए। वित्तीय लेन-देन के लिए हमेशा केवल आधिकारिक और भरोसेमंद ऐप्स का ही उपयोग करना चाहिए और किसी भी डाउनलोड की गई फाइल को पहले अच्छी तरह स्कैन करना चाहिए।

इसके अलावा, अनावश्यक सॉफ्टवेयर को सिस्टम से हटा देना चाहिए और समय-समय पर सिस्टम को अपडेट करते रहना चाहिए। साथ ही, ऑटोमैटिक अपडेट का विकल्प चालू रखना भी सुरक्षित रहता है ताकि सुरक्षा से जुड़े नए अपडेट अपने आप इंस्टॉल होते रहें और साइबर धोखाधड़ी के जोखिम को कम किया जा सके।

ब्राउज़र की हिस्ट्री को नियमित रूप से साफ करना और अपनी लोकेशन साझा करने से बचना भी बहुत आवश्यक है। सोशल मीडिया प्लेटफॉर्म और वेबसाइटों पर दिखाई देने वाली स्पॉन्सर्ड या प्रचार संबंधी सामग्री की सत्यता की जाँच ज़रूर करनी चाहिए। साथ ही, कम से कम 8 अक्षरों वाला मज़बूत पासवर्ड बनाना चाहिए जिसमें अक्षरों, अंकों और विशेष चिन्हों का शामिल हों।

इसके अलावा मल्टी-फैक्टर ऑथेंटिकेशन (MFA) का उपयोग करना और हर अकाउंट के लिए अलग-अलग पासवर्ड रखना अधिक सुरक्षित माना जाता है। अनजान लोगों द्वारा भेजे गए ईमेल, संदेश या लिंक पर क्लिक करने से बचना चाहिए। ऑनलाइन बैंकिंग और खरीदारी के लिए हमेशा सुरक्षित Wi-Fi नेटवर्क का उपयोग करना चाहिए और यदि सार्वजनिक Wi-Fi का इस्तेमाल करना पड़े तो *वर्चुअल प्राइवेट नेटवर्क* का उपयोग करना बेहतर रहता है।

बैंकिंग या अन्य संवेदनशील वेबसाइटों पर *'Remember Password'* विकल्प का चयन करना उचित नहीं माना जाता। महत्वपूर्ण डेटा का नियमित बैकअप लेना चाहिए और उसे किसी सुरक्षित स्थान पर संरक्षित रखना चाहिए। यदि दुर्भाग्यवश कोई व्यक्ति साइबर अपराध का शिकार हो जाता है, तो उसे तुरंत अपने बैंक, पुलिस और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर शिकायत दर्ज़ करानी चाहिए।

सोशल मीडिया पर व्यक्तिगत और वित्तीय जानकारी साझा करने से बचना चाहिए और जल्दी पैसा कमाने का लालच देने वाली योजनाओं या आकर्षक ऑफरों से हमेशा सावधान रहना चाहिए। इन सावधानियों को अपनी दैनिक आदतों में शामिल करके लोग साइबर धोखाधड़ी के जोखिम को काफ़ी हद तक कम कर सकते हैं।

डिजिटल नैतिकता

डिजिटल नैतिकता उन नियमों और सिद्धांतों का समूह है जो डिजिटल तकनीकों और ऑनलाइन गतिविधियों के उपयोग में सही और ज़िम्मेदार निर्णय लेने का मार्गदर्शन करते हैं। इसका उद्देश्य गोपनीयता, सत्यता, जवाबदेही और निष्पक्षता की रक्षा करना है।

आज के समय में, जब जनरेटिव एआई और सोशल मीडिया का प्रभाव तेज़ी से बढ़ रहा है, डिजिटल नैतिकता का महत्व और भी अधिक हो गया है, क्योंकि हर डिजिटल गतिविधि व्यक्ति के मूल्यों और समाज पर प्रभाव डालती है। इसलिए डिजिटल तकनीकों का उपयोग करते समय नैतिक मूल्यों, ईमानदारी और सुरक्षा का ध्यान रखना बहुत ज़रूरी है।

डिजिटल नैतिकता का मुख्य उद्देश्य डिजिटल सेवाओं का सही, सुरक्षित और ज़िम्मेदारी के साथ उपयोग सुनिश्चित करना है। इसी सिद्धांत के अनुसार ऑनलाइन लेन-देन के दौरान *पासवर्ड, वन-टाइम पासवर्ड* (OTP) या *पर्सनल आइडेंटिफिकेशन नंबर* (PIN) किसी के साथ भी साझा नहीं करने चाहिए। इसके अलावा, सोशल मीडिया या किसी भी डिजिटल प्लेटफॉर्म पर आधार नंबर, पैन नंबर, जन्म तिथि या घर का पता जैसी व्यक्तिगत जानकारी साझा करते समय विशेष सावधानी बरतनी चाहिए।

साथ ही व्हाट्सऐप, टेलीग्राम या अन्य सोशल मीडिया माध्यमों पर नफरत फैलाने वाले संदेश, अफवाहें या आपत्तिजनक सामग्री, चित्र और वीडियो उनकी सच्चाई की जाँच किए बिना

आगे नहीं भेजने चाहिए। सरकारी सेवाओं का उपयोग करते समय या कॉमन सर्विस सेंटर के माध्यम से कार्य करवाते समय पारदर्शिता, डिजिटल शिष्टाचार और सम्मानजनक व्यवहार बनाए रखना बहुत आवश्यक है। ग्रामीण भारत में, जहाँ कई बार वित्तीय और डिजिटल साक्षरता सीमित होती है, वहाँ समुदाय के लोगों के लिए यह और भी ज़रूरी हो जाता है कि वे इन नैतिक मूल्यों को अपनाएँ और अपने दैनिक जीवन में उनका पालन करें।

आगे की चुनौतियाँ

अंतरराष्ट्रीय दूरसंचार संघ (ITU) द्वारा प्रकाशित *'ग्लोबल साइबर सिक्योरिटी इंडेक्स'* (GCI) वर्ष 2024 में भारत को टियर-1 श्रेणी का दर्जा मिला है। 98.49 प्रतिशत अंक के साथ भारत अब उन देशों की श्रेणी में शामिल हो गया है जिन्हें साइबर सुरक्षा के क्षेत्र में उत्कृष्ट प्रयासों के लिए जाना जाता है। यह उपलब्धि देश की साइबर सुरक्षा को मज़बूत बनाने की प्रतिबद्धता को दर्शाती है।

हालाँकि, जैसे-जैसे देश का डिजिटल तंत्र तेज़ी से विकसित हो रहा है, वैसे-वैसे साइबर खतरों की जटिलता भी बढ़ती जा रही है। हाल के वर्षों में फिशिंग, रैनसमवेयर, पहचान का गलत इस्तेमाल और यूपीआई तथा ऑनलाइन बैंकिंग से जुड़ी धोखाधड़ी के मामलों में वृद्धि देखी गई है। वर्ष 2024 में लगभग 19.1 लाख साइबर से संबंधित शिकायतें दर्ज की गईं, जो इस प्रणाली में मौजूद गंभीर कमज़ोरियों की ओर संकेत करती हैं।

वर्तमान कानून, जैसे सूचना प्रौद्योगिकी अधिनियम 2000 और डिजिटल पर्सनल डेटा प्रोटेक्शन अधिनियम 2023, एआई आधारित हमलों और डीपफेक जैसी नई चुनौतियों से पूरी तरह निपटने में अभी पर्याप्त नहीं हैं। कृत्रिम बुद्धिमत्ता (AI) आधारित हमलों और डीपफेक जैसी नई चुनौतियों के लिए अभी और प्रभावी प्रावधानों की आवश्यकता है।

भारत के पास साइबर सुरक्षा विशेषज्ञों की कमी है, जिसके कारण धोखाधड़ी में खोए धन को वापस पाने और साइबर अपराधों से प्रभावी ढंग से निपटने की क्षमता प्रभावित होती है। *नेशनल एसोसिएशन ऑफ सॉफ्टवेयर एंड सर्विस कंपनीज़* (NASSCOM) की एक रिपोर्ट के अनुसार भारत को कम से कम 10 लाख साइबर सुरक्षा विशेषज्ञों की आवश्यकता है, जबकि वर्तमान में इस क्षेत्र में काम करने वाले विशेषज्ञों की संख्या लगभग इसकी आधी ही है।

इसके अलावा, आम लोगों में साइबर जागरूकता की भी कमी देखी जाती है। कई लोग फिशिंग संदेश, फर्जी वेबसाइटों या ठगी से जुड़े फोन कॉल को पहचान नहीं पाते। विशेष रूप से ग्रामीण क्षेत्रों में डिजिटल साक्षरता कार्यक्रमों की सीमित उपलब्धता के कारण लोग साइबर अपराधियों के लिए आसान लक्ष्य बन जाते हैं। इसी वजह से ग्रामीण आबादी साइबर धोखाधड़ी के प्रति अधिक संवेदनशील होती जा रही है।

आगे की राह

ग्रामीण समुदायों में डिजिटल साक्षरता बढ़ाने के लिए प्रधानमंत्री नरेन्द्र मोदी ने 'प्रधानमंत्री ग्रामीण डिजिटल साक्षरता अभियान' (PMGDISHA) की शुरुआत की। इस योजना के तहत ग्रामीण लोगों को कंप्यूटर और स्मार्टफोन जैसे डिजिटल उपकरणों का उपयोग करना सिखाया जाता है। इसमें ई-मेल भेजना, इंटरनेट चलाना और ऑनलाइन भुगतान करना जैसी बुनियादी डिजिटल कौशलों का प्रशिक्षण दिया जाता है।

यह योजना खासतौर पर उन ग्रामीण परिवारों को ध्यान में रखकर शुरू की गई है जिनके पास डिजिटल जानकारी नहीं है। वर्ष 2014 के राष्ट्रीय नमूना सर्वेक्षण के अनुसार उस समय ग्रामीण क्षेत्रों में केवल 6% परिवारों के पास ही कंप्यूटर उपलब्ध था।

PMGDISHA का उद्देश्य ग्रामीण क्षेत्रों में डिजिटल जागरूकता और वित्तीय साक्षरता को बढ़ाना है। यह पहल 1 जुलाई 2015 को शुरू किए गए 'डिजिटल इंडिया कार्यक्रम' का भी महत्वपूर्ण हिस्सा है, जिसका लक्ष्य बेहतर डिजिटल अवसंरचना और सुशासन के माध्यम से डिजिटल रूप से सशक्त समाज और ज्ञान आधारित अर्थव्यवस्था का निर्माण करना है।

निष्कर्ष

ग्रामीण भारत में इंटरनेट और डिजिटल तकनीक का विस्तार तेज़ी से हो रहा है और यूपीआई व मोबाइल बैंकिंग जैसी सेवाएँ लगातार लोकप्रिय बन रही हैं। हालाँकि सीमित वित्तीय साक्षरता के कारण मज़बूत साइबर सुरक्षा और डिजिटल नैतिकता की आवश्यकता और अधिक बढ़ गई है। साइबर सुरक्षा हैकिंग और ऑनलाइन धोखाधड़ी जैसे खतरों से सुरक्षा प्रदान करती है, जबकि ग्रामीण आबादी अक्सर फिशिंग और OTP से जुड़े घोटालों का आसानी से शिकार बन जाती है।

डिजिटल नैतिकता शिक्षा, कृषि, वित्तीय सेवाओं और ऑनलाइन सुरक्षा जैसे क्षेत्रों में तकनीक के उपयोग को बढ़ावा देती है और गलत सूचना तथा ऑनलाइन ठगी से बचाव में भी मदद करती है। इस दिशा में मुख्य चुनौतियाँ कम डिजिटल साक्षरता और कमज़ोर सुरक्षा ढाँचा हैं। इन समस्याओं से निपटने के लिए सरकार और निजी संगठन डिजिटल साक्षरता कार्यक्रम और जागरूकता अभियान चला रहे हैं, साथ ही मज़बूत पासवर्ड के उपयोग और संदिग्ध लिंक से सावधान रहने की सलाह दे रहे हैं।

जैसे-जैसे ग्रामीण समुदाय डिजिटल सेवाओं को अपना रहे हैं, साइबर सुरक्षा और डिजिटल नैतिकता के महत्व को समझना बेहद आवश्यक हो गया है। अधिक जागरूकता और प्रशिक्षण से ग्रामीण लोगों का जीवन स्तर बेहतर हो सकता है और साइबर अपराधों में होने वाले नुकसान को कम करके संसाधनों का उपयोग देश के विकास में किया जा सकता है। ❑